Call for tenders EISMEA/2021/OP/0014

GRO/SME/21/12088

Preventing cyber-theft of trade secrets: awareness toolkit for SMEs

Open procedure

TENDER SPECIFICATIONS
# Table of Contents

1 SCOPE AND DESCRIPTION OF THE PROCUREMENT ......................... 4

1.1 Contracting authority: who is the buyer? .................................. 4

1.2 Subject: what is this call for tenders about? ................................ 4

1.3 Lots: is this call for tenders divided into lots? ............................ 4

1.4 Description: what do we want to buy through this call for tenders? ......... 4

1.4.1 Background and objectives ................................................... 4

1.4.2 Detailed characteristics of the purchase .................................... 11

1.4.3 Intellectual Property Rights .................................................. 20

1.4.4 Confidentiality and Data Protection ........................................ 20

1.4.5 Performance and quality requirements ...................................... 21

1.4.6 Deliverables ........................................................................... 22

1.4.7 Meetings ............................................................................... 25

1.4.8 Indicative timetable .................................................................. 25

1.5 Place of performance: where will the contract be performed? .............. 26

1.6 Nature of the contract: how will the contract be implemented? ............... 26

1.7 Volume and value of the contract: how much do we plan to buy? .......... 27

1.8 Duration of the contract: how long do we plan to use the contract? ........ 27

1.9 Electronic exchange system: can exchanges under the contract be automated? .............................................................................. 27

2 GENERAL INFORMATION ON TENDERING ................................. 28

2.1 Legal basis: what are the rules? .................................................... 28

2.2 Entities subject to restrictive measures and rules on access to procurement: who may submit a tender? .................................................. 28

2.3 Registration in the Participant Register: why register? ......................... 29

2.4 Ways to submit a tender: how can economic operators organise themselves to submit a tender? .................................................. 30

  2.4.1 Joint tenders .......................................................................... 31

  2.4.2 Subcontracting ....................................................................... 31

  2.4.3 Entities on whose capacities the tenderer relies to fulfil the selection criteria .............................................................................. 33
3 EVALUATION AND AWARD .................................................................................. 34
3.1 Exclusion criteria ............................................................................................. 34
3.2 Selection criteria .............................................................................................. 35
  3.2.1 Legal and regulatory capacity ..................................................................... 36
  3.2.2 Economic and financial capacity ................................................................. 36
  3.2.3 Technical and professional capacity ............................................................ 38
3.3 Compliance with the minimum requirements of the procurement documents ................................................................................. 43
3.4 Award criteria .................................................................................................. 44
3.5 Award (ranking of tenders) .............................................................................. 46
4 FORM AND CONTENT OF THE TENDER .......................................................... 48
  4.1 Form of the tender: how to submit the tender? .............................................. 48
  4.2 Content of the tender: what documents to submit with the tender? ........... 48
  4.3 Signature policy: how can documents be signed? ........................................ 50
  4.4 Confidentiality of tenders: what information and under what conditions can be disclosed? .............................................................................. 50
5 APPENDIX: LIST OF REFERENCES .................................................................. 52
6 ANNEXES ........................................................................................................... 53
1 Scope and description of the procurement

1.1 Contracting authority: who is the buyer?

This call for tenders is launched and managed by the European Innovation Council and SMEs Executive Agency (EISMEA)\(^1\), referred to as the *Contracting Authority* for the purposes of this call for tender, acting under the powers delegated by the European Commission (here after “EC”, “Commission” or “the Commission”).

1.2 Subject: what is this call for tenders about?

The subject of this call for tenders is: “Preventing cyber-theft of trade secrets: awareness toolkit for SMEs”, as indicated in Heading II.1.1 of the contract notice.

1.3 Lots: is this call for tenders divided into lots?

This call for tenders is not divided into lots.

1.4 Description: what do we want to buy through this call for tenders?

The services that are the subject of this call for tender, including any minimum requirements, are described in detail below.

Variants (alternatives to the model solution described in the Tender specifications) are not allowed. The *Contracting authority* will disregard any variants described in a tender.

1.4.1 Background and objectives

Background

a) Introduction

Competitiveness through innovation is to a large extent dependent on intangible assets such as know-how and trade secrets. These are being targeted by industrial espionage and theft through cyber means by private and state-sponsored actors. This causes loss of

\(^1\) EISMEA was established by the Commission Implementing Decision (EU) 2021/173 of 12 February 2021: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0173](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0173). EISMEA succeeds and replaces the former EASME. Any reference in this document and its annexes to EASME is to be understood as a reference to EISMEA.
competitiveness (loss of contracts, loss of sales) and have negative impact on innovation, with increased cybersecurity costs as well as financial and reputational damages for companies. The negative economic impact of intellectual property (IP) cyber-theft is likely to increase even more with the development of the data economy and the digital transition.

Estimates show that cyber-enabled theft of trade secrets currently account for nearly EUR 60 billion losses in economic growth in Europe and a consequent potential loss of 1,000,000 jobs. According to a recent study\(^2\), 94% of cyber-attacks in manufacturing, Information and Communication Technologies (‘ICT’), health and financial sectors are driven by industrial espionage, while the average time from the intrusion to its detection is 469 days in Europe\(^3\).

Innovative small and medium-sized companies and start-ups often poorly protect information on ongoing contract negotiations, customer and marketing information, data, new product designs and R&D plans, which all can constitute trade secrets or confidential business information. This is particularly true in the online environment.

The Commission announced initiatives to improve the resilience of EU small and medium-sized enterprises (SMEs) and research community against cyber-theft of IP, in particular trade secrets, in the Communication “Making the most of the EU’s innovative potential: An intellectual property action plan to support the EU’s recovery and resilience”\(^4\) of 24 November 2020.

Given the nature of the growing cloud industry and the number of cloud-based services, companies increasingly use cloud computing\(^5\). Cloud computing\(^6\) offers businesses attractive cost-saving opportunities, which may include storing trade secrets in the cloud. This leaves businesses at risk of losing valuable trade secrets if relevant cybersecurity risks are not appropriately addressed. An entire business strategy could be hacked, downloaded and handed over to a competitor or a foreign government.

The protection of valuable data must also be ensured. Among industrial and commercial data created by European businesses and research organisations there is much commercially valuable information and trade secrets. The European Union is investing heavily in the digital transition. Among other initiatives, the EU is going to co-create a protected framework to allow the use of data, the European Open Science Cloud

---


\(^3\) The scale and impact of industrial espionage and theft of trade secrets through cyber. PWC for DG GROW, 2018 – Study commissioned by the Commission which conclude to a lack of awareness of EU SMEs about cybertheft. With these terms of reference (TORs) the Commission responds to the call for improving business awareness about the problem. [https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en](https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en)


\(^5\) The opportunity to save money that would otherwise be spent on acquisition or development costs, maintenance, or physical storage of software, servers, and data storage. From a systemic perspective, increasing use of cloud computing by the industry could also open reflections on the risk allocation and transparency through the creation of national standards for cybersecurity and how potential risks may affect a user’s competitive assets like trade secrets.

\(^6\) Whether that refers to data storage or service models like Software as a Service (SaaS).
The European Open Science Cloud (EOSC)\(^7\), where every researcher will be able to better use not only their own data, but also those of others, to come to new insights, new findings and new solutions. Given the ever-increasing importance of data, protecting them from cyber-misappropriation is thus nowadays even more crucial than before.

Yet, cyber theft activities of private and state actors are increasing. Cyber-theft of IP is a concrete, growing and multifaceted reality, where the vulnerability of one player can have important consequences on other players across the supply/value chain.

SMEs are exposed to cyber-attacks and data-leaks as much as larger companies, but they usually display lower awareness about the threats and are less prepared and equipped to deal with their consequences.

In a global economy, the threat and continuing misappropriation of trade secrets often involves various actors in sophisticated multinational schemes, conspiracies and organised criminal enterprises often working for or supported by foreign governments conducting systematic industrial espionage.

As the EU 5G Toolbox\(^8\) explains, the increased virtualisation of networks\(^9\) and larger attacker surface due to more potential entry points for attackers, might bring additional incentive to target 5G networks by organised crime groups, corporate entities seeking to gain competitive advantage in the technological field through IP theft.

However, **cyber-theft of trade secrets can also happen during daily working operations** of companies, e.g. in the case of incautious treatment of confidential information by managers/employees or stealing of trade secrets by disgruntled employees.

Restricting access to trade secrets through enforcing cybersecurity protocols requires companies to gauge the value and risk behind it. However, matching investments and risks in cybersecurity and trade secret protection is difficult, and cybersecurity is most often perceived as a cost rather than a revenue-producing investment. Meanwhile technology and cyber-attacks continues to develop, as the effectiveness of security decreases over time.\(^10\)

Therefore, the kind and level of risk that companies will be able to accept in the near future should determine the mitigation strategies but also the instruments that the EU policy can put in place to help companies manage the risk.

Trade secrets are also used as a pre-Intellectual Property Rights (IPR) protection tool. For instance, pre-filing patent information is usually kept secret. As regards copyright,
even if the protection arises with the creation of the work, protecting the confidentiality of preparatory works remains key to avoid losses or misappropriation of rights.

Either as specific choice or as a pre-IPR protection tool, trade secrets are usually more vulnerable to cyber-misappropriation.

There is a need to enhance the level of awareness and quality of response by SMEs, start-ups and research organisations to trade secret theft attempts, particularly in those EU industries that are more likely to be targeted by industrial espionage (because of their technological edge or strategic value for a third country’s national development strategy).

SMEs and innovative start-ups are often part of interconnected systems, and their weak cybersecurity/IP management preparedness might have a negative impact also on the protection of trade secrets belonging to larger companies in the value chain, thus discouraging cooperation or exposing to potential misappropriations.

While aiming at improving the quality of cybersecurity practices, existing public awareness initiatives on cybersecurity for SMEs at the EU or national level do not specifically address the issue of trade secrets misappropriation through cyber-means.

The SME IP Helpdesks of the EU provide general information about cybersecurity regulations and protection of trade secrets in the digital environment. However, the relevant services and information are addressed to the wide SME audience in the EU or in a specific non-EU country and – for various reasons – do not delve into the structural, managerial and technical aspects underpinning an effective corporate policy to counter cyber-theft of trade secrets.

At Member States’ level, there are few government-funded educational campaigns or business-led initiatives targeting the issue of cyber-theft of trade secrets. They generally merely limit themselves at issuing good practice and are often limited to specific industry sectors.

**b) The Trade Secrets Directive**

The Trade Secrets Directive has introduced a common set of rules for civil law measures of redress across the European Union, which include a common definition of trade secrets, provisions on precautionary measures, injunctions, calculation of damages and protection of confidentiality during court proceedings.

According to the Directive, ‘trade secret’ means information, which meets all of the following requirements:

(a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) it has commercial value because it is secret;

---


12 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure
(c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

In general, any confidential business information, which provides an enterprise a competitive edge and is unknown to others may be protected as a trade secret. Trade secrets encompass both technical information, such as information concerning manufacturing processes, pharmaceutical test data, designs and drawings of computer programs, and commercial information, such as distribution methods, list of suppliers and clients, and advertising strategies.

The Trade Secrets Directive has also triggered additional awareness in the private sector, at least in some large multinationals\textsuperscript{13}, about the importance of putting in place serious corporate policy to counter or mitigate the risk of cyber-theft of trade secrets.

In this respect, ensuring consistent interpretation by national courts of the “reasonable steps” for protection required by Article 2 of the Directive, would be conducive to supporting good cybersecurity practices by trade secrets holders. There is a logical and strategic link between the reasonable steps and the cybersecurity measures.

Whether a company has put forth reasonable efforts to maintain the secrecy of its information is to be determined based upon the circumstances. Determining the level of reasonable protection is ultimately down to the courts, and adds another layer to the interaction between policy and a firm’s cybersecurity spending decisions.

Since trade secrets lose their protected status as such once they become generally known or readily accessible, the more valuable a trade secret, the more extensive the efforts should be to protect it\textsuperscript{14}\textsuperscript{15}.

c) Cybersecurity & IP awareness, standards, insurance

Cyber-theft of trade secrets as valuable intangible assets could be drastically reduced by promoting cybersecurity and IP management awareness at all levels, both in daily business practices and in the interface with customers and business partners. Putting in place smart corporate policies to protect one’s proprietary know-how, including measures to counter cyber industrial espionage, could avoid huge economic losses.

To this purpose, the European Commission’s IP Action Plan of November 2020 envisages that future awareness actions should focus on how to improve the resilience and capability of European SMEs to identify and classify trade secrets, detect misappropriation attempts and respond to control the damage.

The development and adoption of international cyber security standards is generally considered a valuable tool for the business world to prevent cyber theft of trade secrets or mitigate its consequences. However, the development of international standards is a long process and require a breadth of large international efforts.

\textsuperscript{13} Fourth Brand Protection Congress, 4 December 2019, Frankfurt (Germany). Presentation by Thyssenkrupp
\textsuperscript{14} Nicola Searle, Trade secrets in the wild (Part 1): some economics of cybersecurity investment, the IP KAT, March 2021
\textsuperscript{15} In that regard, the use of cloud computing presents additional challenges, as information can be more easily transferred between parties.
In this respect, “informal standards” in the form of best practices developed by larger companies to protect proprietary know-how from cyber-misappropriation can help develop guidelines in support of smaller players.

As companies purchase insurance policies to improve their security and reduce their expected losses from attacks, insurance companies can also play a role in developing best practices in that respect and encourage companies to adopt those practices to reduce their premiums (or as a precondition to coverage).

**d) Existing awareness initiatives (examples)**

The EU’s efforts to upskill the workforce, to develop, attract and retain the best cybersecurity talent and to invest in world class research and innovation, form an important component of protection against cyber threats generally. The revised Digital Education Action Plan\(^{17}\) will raise cybersecurity awareness among individuals, especially children and young people, organisations and businesses, including SMEs.

Multiple initiatives exist at **EU level**:

The **EU IP SME Helpdesk** and the International IP Helpdesks offer first information and guidance to SMEs on IP related issues, including protection of trade secrets.

The **IP pre-diagnostic** services are offered to SMEs that submitted a proposal to the H2020 SME Instrument or the EIC Accelerator\(^{18}\). The relevant services in the European Union Intellectual Property Office’s (EUIPO’s) SME Fund\(^{19}\) and other EUIPO training programs can also help audit trade secrets protection capabilities of SMEs.

The **Leadership4SMEs**\(^{20}\) is another EU funded project for the development of support services to leverage SME’s IP as a strategic asset for access to finance.

The **Intellectual Property Booster (IP Booster)**\(^{21}\) is a specialised professional IP service for public research organisations looking to realise value from their research results. IP experts examine business cases and guide towards the best intellectual property strategy, at no cost and fully supported by the European Commission.

The **European Cybersecurity Month** (ECSM) is the European Union’s annual campaign conducted by the European Union Agency for Cybersecurity (ENISA) and dedicated to promoting cybersecurity among EU citizens and organisations, and to providing up-to-date online security information through awareness raising and sharing of good practices.

**At national level**, examples of cybersecurity awareness initiatives that support SMEs include Germany’s Federal Office for Information Security's (BSI) Basic IT-
Protection\textsuperscript{22} or Belgium’s Centre for Cybersecurity’s Guide for SMEs\textsuperscript{23} and the Netherlands’ Digital Trust Centre. National business organisations like VDMA\textsuperscript{24} (German companies and SMEs in the mechanical engineering sector), have developed sector-specific studies and guides\textsuperscript{25} on product piracy and trade secret theft.

Finally, ENISA\textsuperscript{26} acts as the EU center of expertise for cybersecurity. In this role, it provides information about technologies like Internet of Things (“IoT”), big data and IT infrastructure. Since 2008, ENISA has provided cybersecurity training material for specialists that cover technical, operational and legal domains. Each domain has several topics and courses. ENISA has developed several tools and training material specifically for SMEs, such as the Cloud Security Guide for SMEs.

**Objectives (General and Specific)**

The objectives of the contract is to set-up awareness raising tools to help EU SMEs and the research community to fight cyber theft. For this purpose, a hands-on IP cyber-theft prevention Toolkit is to be produced. The contractor will develop and upgrade existing awareness raising tools and define awareness raising campaigns for SMEs and the research community holding trade secrets and confidential business information\textsuperscript{27}. When relying on existing tools, the contractor shall take into account possible issues with copyrights. The Commission may support the contractor in obtaining the permission to use. To the extent that new tools could be introduced, the contractor will develop them. The contractor will also design an online portal (concept and content) and other educational resources that will help EU SMEs enhance their resilience and preparedness with respect to the risk of misappropriation of trade secrets through cyber means. That portal might eventually be linked to/integrated with future EUIPO’s online resources for SMEs. The contractor shall also provide recommendations with regard to additional and/or new initiatives that could be undertaken by the Commission, including on cybersecurity certification schemes and standards, cyber-insurance and others of relevance.

The main purpose of the IP cyber-theft prevention Toolkit will be to fill gaps and/or upgrade existing awareness instruments, with the view to promote a European business culture of cyber-secure IP management and IP-aware cybersecurity.

In addition, the contractor will have to develop a strategy on how to maximize the dissemination and accessibility (also in terms of business-friendly language) of the IP cyber-theft prevention Toolkit, in particular on how to reach the most vulnerable owners of trade secrets, but also intermediaries and service providers who can function as multipliers.

\textsuperscript{22} https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
\textsuperscript{24} The Mechanical Engineering Industry Association (Verband Deutscher Maschinen- und Anlagenbau – VDMA)
\textsuperscript{25} https://www.vdma.org/cybersecurity
\textsuperscript{27} For the purpose of this contract, any reference to IP will be construed as trade secrets and confidential business information. Any reference to trade secrets should be considered as including confidential business information.
**Input by the Contracting Authority:** The Contracting Authority will provide the contractor with relevant previous studies conducted in the field of trade secrets protection and commissioned by the Commission. The Contracting Authority will also make available relevant information in its possession, in particular:

- The study “The scale and impact of industrial espionage and theft of trade secrets through cyber”, PWC for DG GROW, 2018 – Study commissioned by the Commission which conclude to a lack of awareness of EU SMEs about cyber-theft.  
- IP awareness raising tools developed by the international IP SME Helpdesks of the EU
- ENISA’s cybersecurity awareness campaigns and materials

**1.4.2 Detailed characteristics of the purchase**

**Geographical scope**

The implementation of the contract shall cover all EU Member States and at least the following third countries: the United Kingdom (UK), Japan, Singapore, Taiwan, Australia, Canada, New Zealand and the United States of America (USA).

**Description of tasks**

Taking into account existing awareness initiatives developed in the EU and its Member States, and benchmarks from similar initiatives developed in third countries, the contractor will have to define the scope of the work and provide the rationale of the sectoral awareness raising tools and actions.

The contractor will also have to map and further define the initiatives that should become part of the IP cyber-theft prevention Toolkit.

In a forward-looking perspective, the contractor must also recommend actions and methodologies to keep the Toolkit up-to-date, and must propose reasonable and specific indicators to monitor its performance and impact over time as well as its dissemination.

**Task 1: Research**

**Task 1.1: Identification of the problem**

Building on the available literature, the contractor must prepare an introductory report that will offer an overview of the industry practices and must identify at least three “use cases” for each target sector (see below), to describe the most common patterns and features of IP cyber-theft. This report must:

---

- describe the specific aspects and data sharing sensitivities to be addressed from a cybersecurity and an IP management perspective;

- articulate which industry sectors are most exposed to the threat and explain the main underlying reasons;

- identify the criteria that influence cyber theft (e.g. internet infrastructure, geo location, relative isolation of the businesses or presence in a cluster, IP management, etc.). An EU mapping must be drawn up.

The contractor must draw its findings and analysis also from an EU-wide review of national case law concerning judicial interpretations of Directive EC/943/2016 – particularly the steps reasonably required to ensure secrecy whenever cyber-misappropriation is at stake.

The contract must cover five industry sectors at EU and national levels. Three of them must be: semiconductors, biotechnologies and the defence industry. The remaining two sectors must be proposed in the offer and duly justified, taking into consideration (a) their importance for the EU recovery and resilience, (b) their role in the value chains of the EU industrial ecosystems and IPCEIs (Important Projects of Common European Interest), in light of inherent risks of being more exposed to IP cyber-theft.

**Task 1.2: Mapping of existing awareness raising initiatives**

The contractor must prepare a report that will include a mapping review of existing public awareness instruments and initiatives in the EU, addressing IP and cybersecurity from the public and private sector.

The report will include critical inputs to the Commission in order to identify possible margins for improvement, when this seems desirable.

**Task 1.3: Identification of existing good practices**

The contractor must conduct surveys and interviews to identify existing good practices to manage and mitigate the risk of trade secrets cyber-misappropriation, adopted by large corporations, associations or service providers in the cybersecurity and IP consulting sectors.

Surveys and interviews shall be conducted in the beginning of the contract duration so that results can be analysed and provide grounds for developing the Toolkit.

Building on the available evidence/literature and through reaching out to industry experts, the contractor shall carry out at least 15 structured/semi-structured interviews in each target sector (at least 75 interviews in total) across at least 10 EU Member States. These will investigate the existing good practices to manage and mitigate the risk of cyber-misappropriation of trade secrets, adopted by large corporations and service providers in the cybersecurity and IP communities.

---

31 Other sectors of possible interest: automation/robotics, transport equipment (rail, air, autonomous vehicles), chemicals

32 [https://clustercollaboration.eu/in-focus/industrial-ecosystems](https://clustercollaboration.eu/in-focus/industrial-ecosystems)

33 The contractor shall also keep into consideration the findings of the study on the scale and impact of industrial espionage and the theft of trade secrets through cyber (PWC for DG GROW, 2018) [https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en](https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en)
The tenderers must already show in their tenders the potential interviewees/companies/organisations that they have identified, which are most likely to provide meaningful inputs.

The final list of interviewees should be based on their knowledge of the subject and will be agreed with the Commission services and EISMEA at the implementation stage.

The Commission and/or EISMEA may issue a recommendation letter that the contractor will be able to present to approached stakeholders.

In conducting the interviews/survey the contractor shall respect the applicable data protection rules at national and EU levels and ensure privacy is respected (please see section 1.4.4 of these tender specifications).

Task 1.3 must cover:

- Elaborating a questionnaire (to be approved by the Commission services and EISMEA) for carrying out survey and structured interviews with corporate experts[^34] in the field of cybersecurity and IP.
- Devising a fielding strategy which should allow obtaining a critical number of interviews from the five target sectors;
- Carrying out and complete a minimum number of 75 in-depth interviews (face-to-face or by video-conference/telephone) across at least 10 Member States. The geographical coverage should be balanced and ensure representativeness among Member States (i.e. more interviews should come from highly populated countries/with larger presence of industries in the target sectors);
- Collecting the replies/inputs from the interviews and presenting descriptive statistics of the results (e.g. number and characteristics of the interviewees, sectors, etc.);
- Analysing the results and drafting an in-depth assessment report, on the basis of concrete examples and use cases. In this respect, the analysis should also highlight correlations and emerging patterns in the good practices identified. The report should also include in its annex the minutes of the interviews[^35];
- Preparing a five-pages report to draw conclusions on ‘how’ businesses can effectively counter cyber-misappropriation of trade secrets in their daily operations.

Research questions/topics for the interviews will include (non-exhaustive list, to be further developed in the offer):

- Corporate policies to conduct dedicated risk assessments and define the most important business choices and actions to improve resilience;
- Methods to identify and protect trade secrets and confidential business information;

[^34]: To avoid oriented results the tender should describe the selection method depending on neutral factors such as the population (e.g. interviewees’ sample selected randomly)
[^35]: Personal data shall be treated in accordance to Regulation (EU) No. 2018/1725
• In-house corporate practices to prevent cyber-misappropriation;
• Measures that allow to detect and respond to cyber-threats aimed at acquiring trade secrets and react;
• Measures to protect trade secrets and confidential business information in the context of corporate IP strategies and business relationships with third parties including research and academic institutions
• Available options to recover the loss (damage control) when misappropriation has occurred.

Deliverables of Task 1 are:

Task 1.1:
Introductory report identifying the problem. The report must identify five target sectors and three use cases per sector.

Task 1.2:
A report providing a mapping of existing public awareness initiatives and instruments as well as recommendations for improvement.

Task 1.3:
- A questionnaire;
- A fielding strategy: list of businesses to contact, timeline, refined fielding the strategy to achieve the minimum target number of responses;
- Raw results: Written summary of in-depth interviews;
- Quantitative and qualitative exhaustive descriptive statistics;
- A report on good practices, which must include an in-depth assessment based on the analysis of the results, concrete examples and use cases;
- Conclusions on means for businesses to effectively counter cyber-misappropriation of trade secrets in their daily operations.

Task 2: Develop an IP cyber-theft prevention Toolkit

The results of the work under Tasks 1.1, 1.2 and 1.3 above, and in particular the survey and interviews and further discussions with the Commission, shall form the basis for developing the Toolkit.

Recital 45 of the NIS 2 Directive (Commission proposal COM(2020) 823 final of 12.12.2020) (45) Entities should also address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem. In particular, entities should take appropriate measures to ensure that their cooperation with academic and research institutions takes place in line with their cybersecurity policies and follows good practices as regards secure access and dissemination of information in general and the protection of intellectual property in particular. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures.
Under Task 2, the contractor must develop:

2.1 A set of jargon-free and actionable sectoral awareness raising tools for SMEs and the research community. The tools shall be fine-tuned to the economic sector concerned and may have ramifications per (group of) Member States. The contractor will primarily analyse existing awareness raising materials available for SMEs and may suggest improvements;

2.2 Content of 5 training modules

2.3 Testing of training modules

2.4 Concept and content of online portal and social media outreach.

The above-mentioned sub-tasks are further detailed below:

**Task 2.1: Sectoral awareness raising tools**

- The contractor must prepare a set of integrated awareness raising tools that shall include as a minimum:
  - Business guides (at least one per industry sector) that can either be a (a) new state of the art sectoral guide and/or (b) updates/upgrades of existing ones;
  - List of frequent questions and answers raised by the private sector concerning the protection of trade secrets in the cyber space (customised by sector);
  - Case studies on good practices (at least three per industry sector) and integrate them as part of training and e-learning activities;

The contractors shall suggest additional tools, such as webinars, video testimonials or podcasts and outline follow up steps to keep the awareness raising tools up-to-date.

These should be easy to replicate and adapt to different portals and national contexts, where suitable. Tenderers are free to add other content if relevant.

**Task 2.2: Content of training modules addressed to managers and employees**

The contractor must develop five pilot training modules for hybrid (online and/or on-site) workshops learning. The contractor must provide the content of the modules. Each training module must cover a different theme and/or sector, to be agreed with the Commission and EISMEA. The training modules must be in the form of seminars/webinars in English.

A short explanatory video with instructions for the users of the module must accompany each module. The tenderer must propose a minimum number of hours of training.

The contractor will also develop a strategy for future delivery of the learning tools, ensuring cost-effective, convenient outreach to SMEs regardless of their location. The strategy should address the following aspects (non-exhaustive list):

- Creating synergies among existing awareness raising initiatives;
- Reaching critical mass of target audience;
- Intensifying contact with the target audience, also through cooperation with SME intermediary groups, e.g. consultants, business associations, etc.;
- Reaching out at SME target groups that are not members of intermediary organisations;
- Offline and online marketing;
- Technical features and possible constraints.

**Task 2.3: Testing of the pilot training modules**

The training modules must be tested by the European IP Helpdesk and if applicable other organisations relevant to the subject of the call which will be agreed with the Commission and EISMEA in order to collect sufficient feedback. For this purpose, the Commission and EISMEA will facilitate the contact with the European IP Helpdesk. A report on the testing results must be also prepared.

**Task 2.4: Concept note for an online information portal**

Business guides, e-learning modules and case studies (e.g. the awareness material) will be in the future made available on a dedicated portal for public use free of charge.

The online information portal should allow for an intuitive understanding of ‘what’ to find ‘where’.

The contractor must develop a detailed concept note for a portal. This will be a concept for a portal to be included either on a stand-alone website or as a section of existing websites of the EU institutions/agencies to avoid duplications.

The concept note must include:

- What would be the content of the portal: type, purpose and expected results of the services offered;
- The proposal for a design (architecture) of the portal;
- Analysis of pros and cons of each solution (e.g. stand-alone website vs section of existing webpage);
- Development, maintenance and update of the portal/website.

**Deliverables of Task 2 are:**

**Task 2.1:**

- Sectoral business guides;
- List of FAQ;
- Case studies of good practices;
- Report on additional tools

\textit{Task 2.2:}

- An integrated strategy/methodology for future delivery of training modules;
- Content of 5 training modules;

\textit{Task 2.3:}

- Report on results of testing of training modules

\textit{Task 2.4:}

- Detailed concept note for a web-portal

\textbf{Task 3: Strategy for dissemination and policy recommendations}

\textbf{Task 3.1: Strategy for dissemination}

The contractor must first of all develop a strategy on how to disseminate the toolkit so that the targeted audience is reached both at EU and national level (multi-lingual approach). Particular attention should be given to educational institutions and business schools, research communities and SMEs/business associations. The dissemination strategy must include potential partners and multipliers for future actions by the Commission.

The contractor must also outline social media programs with dedicated profiles on the most popular professional platforms and social media.

Particular attention must be given also to possible incentives for knowledge sharing by larger companies to SMEs.

The contractor must also outline (reasonable) quantitative and qualitative key performance indicators (KPIs) that should allow to monitor the impact of the overall awareness raising action described in this document. The KPIs must be approved by the Commission and EISMEA.

\textbf{Task 3.2: Policy Recommendations}

Finally, the contractor must provide policy recommendations with regards to additional initiatives that could be undertaken by the Commission, including initiatives on reporting mechanisms for improving situational awareness objectives and instruments\(^ {37} \), certification schemes and standards, cyber-insurance and others of possible relevance.

\textit{Deliverables of Task 3 are:}

- Strategy on the dissemination of the Toolkit;
- A report including an outline of social media programs, an outline of KPIs to monitor the impact of awareness raising actions and policy recommendations.

**Task 4: Validation workshop**

The contractor will organise a validation workshop to present the results of Tasks 1, 2 and 3 and seek feedback from the participants.

This workshop will take place in online format from Brussels and will aim at discussing the work conducted, which will be presented by the contractor. The Commission, together with the contractor, will identify the participants in the event and may decide to invite additional speakers. Approximately 300 experts in the area of cyber-security, both from private and public sector will be invited to the workshop. Experts from the five sectors (i.e. semiconductors, biotechnologies, the defence industry and the two other sectors the contractor will select) need to be properly represented at the workshop. The final number of participants should be around 200. The workshop should be 3 to 5 hours long.

Upon receiving feedback, the deliverables (mainly the Toolkit, dissemination strategy and policy recommendations) will be fine-tuned to take on board the comments of workshop’s participants.

At the workshop, the contractor should present the draft results of the work. The details of the presentation will be agreed in advance between the contractor and the Commission.

The contractor must submit within 2 weeks after the workshop a report on the event, taking into account the relevant results and minutes of the workshop.

*Deliverable of Task 4 is:*

- Report on the event

**Methodology and coordination**

The technical offer shall comply with the technical specifications and provide, as a minimum, the information specifically requested. To this end, the contractor is expected to collect, analyse, judge and present primary and secondary data, consult the relevant public and private stakeholders or perform other form of public or targeted survey, interviews, focus groups, workshops, etc.

The contractor shall conduct all tasks in the context of the objectives set out above, taking into account the previous analyses done on this topic by the Commission, other EU institutions as well as available information from public and private stakeholders at international, EU, national and regional level. The contractor shall also take into account the existing relevant policy and legislative framework previously described.

The contractor shall ensure robustness of information by trying to acquire it from more than one source. In particular, findings from interviews and consultations should be complemented when possible by official statistics and studies.

The contractor must support findings and recommendations by explaining the degree to which these are based on opinions, analysis and objectively verifiable evidence. Where opinions are the main source, the degree of consensus and the steps taken to test the opinions should be given.

The offer must be developed following a clear and detailed methodology, covering all aspects of the tender specifications.

The tenderer must propose its specific methodology, taking into account the context and objective of the tender and the minimum tasks and requirements indicated in the section 1.4.2 of these tender specifications.

The final deliverables, as explained in details in section 1.4.6, will be a written final report and annexes, which must cover all the tasks explained in the present section according to the methodology explained in detail.

More generally, the works should be based on data from a variety of sources such as e.g. company, industry, government, trade journals and organisations, as well as available market studies, including any relevant Commission study. It should include information from literature reviews and discussions/interviews with technology/market experts and key stakeholders.

Efficient use of available networks should be made by liaising with relevant stakeholder groups. The contractor, EISMEA and DG for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) will work in close co-operation. In practice, this means that the contractor must be ready to deliver, when requested, information on the work progress.

Green Public Procurement and events

In line with the Directive 2004/18/EC of the European Parliament and of the Council on the award of public services contracts, tenderers are expected to describe any action they envisage for environment and energy efficient solutions, incorporating these concerns into all aspects of service delivery and infrastructure management.

The services provided by the Contractor must contribute to the Commission's commitment to minimise the environmental impact of its everyday work and continuously improve its environmental performance by integrating environmental criteria into its procurement procedures and organisation of events.

Services need to fulfil a number of standards as to the ethical, social and environmentally friendly origin, production, delivery and distribution of the materials. The principles and strategies linked to the sustainable use of natural resources, waste prevention and recycling will be taken into account. Examples of proofs/labels: compliance with EMAS, ISO 14 001, EU Ecolabel, and other ISO type I label, equivalent labels and standards, etc. Further information and guidelines can be found in
Tenderers will take into account the “Guidelines on organising sustainable meetings and events at the Commission”

The contractor is encouraged to reduce the environmental impact of events or meetings by: choosing venues easily accessible by public transport, proposing accommodation options in certified environmentally friendly hotels, proposing travel itineraries using carbon-offsetting flights or trains (instead of flights), proposing green catering (prefer plant-based food, opt for seasonal and organic food and drinks, avoid food waste and single use plastic, and provide reusable cups/bottles/glasses/cutlery/plates), pay attention to the management of waste and place displays to communicate the sustainable arrangements that have been put in place.

The contractor is encouraged to consider measures for the performance of the tasks under the contract, which increase the social impact of the contract. For instance, this could involve recurring to operators working on the professional integration of disadvantaged persons, women, and long-term unemployed people or considering accessibility for all solutions, facilitating the participation of people with disabilities.

1.4.3 Intellectual Property Rights

The intellectual property rights related to the services/studies are foreseen in Articles I.10 and II.13 of the draft service contract.

Parts of results pre-existing the contract

If the results are not fully created for the purpose of the contract this should be clearly pointed out in the tender. Information should be provided about the scope of pre-existing materials, their source and when and how the rights to these materials have been or will be acquired.

Plagiarism in the tender

In the tender all quotations or information originating from other sources and to which third parties may claim rights have to be clearly marked (such as: source publication including date and place, creator, number, full title etc.) in a way allowing easy identification.

1.4.4 Confidentiality and Data Protection

Confidentiality is required of all persons working or collaborating directly or indirectly in the performance of tasks following this call for tender, as they might come into contact with confidential information during the course of their work. Any breach of confidentiality will be treated as professional misconduct and could lead to the termination of the contract as set out in Article II.5 of the draft service contract.

Specific requirements relating to personal data and the protection thereof are set out in the draft service contract. The contractor is equally responsible for ensuring the
application of this obligation in respect of any of his/her direct or indirect sub-
contractors.

The contractor will ensure compliance with the applicable data protection rules at
national and EU levels, including:

(1) the Regulation (EU) 2018/1725 of the European Parliament and of the Council of
23 October 2018 on the protection of natural persons with regard to the processing
of personal data by the Union institutions, bodies, offices and agencies and on the
free movement of such data\(^{40}\) and

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)\(^{41}\).

During the contract implementation, the contractor must comply with the Contracting
authority’s personal data protection procedures, including models of data protection
notice (e.g. for the website, event, survey, etc.) provided by the Contracting authority,
and with the general and specific contractual clauses I.9.2 and II.9.2, when processing
personal data of stakeholders on behalf of Contracting authority.

The contractor will cooperate with the Contracting authority in ensuring that personal
data is handled lawfully and if required not without explicit prior consent of the subjects
involved (e.g. beneficiaries and their subcontractors).

It is the contractor’s responsibility to make sure the necessary permission/agreements
for taking pictures and filming have been obtained by the participants prior to the
events.

Image rights disclosure forms have to be provided to and collected from the participants
by the contractor via the registration/application process.

In addition, the contractor will ensure that personal data is processed and accessible
only within the territory of the European Union and the European Economic Area and
will not leave that territory. Access to data may be given on a need to know basis only
to authorised persons established in a country, which has been recognised by the
European Commission as providing adequate protection to personal data.

All websites, platforms, digital applications and online registration forms containing
personal data must be hosted within the European Union and abide by the same legal
obligations on personal data protection as provided in Article I.9.2 of the draft service
contract.

1.4.5 Performance and quality requirements

All deliverables under this contract will be assessed on the basis of the following quality
criteria, and rated (poor/satisfactory/good/very good/excellent) in relation to the
following aspects:

\(^{41}\) https://eur-lex.europa.eu/eli/reg/2016/679/oj
(1) **Relevance**: The reports, questionnaires, guides, methodology and FAQs must include relevant and adequate measures to ensure a concrete and efficient setting-up and implementation of the Toolkit, and its uptake by SMEs and the research community. The dissemination strategy must be relevant in view of current communication strategies (including on social media) and in view of the objective, that is to raise awareness among SMEs and the research community.

(2) **Appropriate design**: All trainings, webinars and learning modules must have an appropriate design and effective organisation. An appropriate design includes activities and actions that are fit for purpose, involve the participants in an interactive way and meets the objectives set out in this Call. These must be reflected in the strategy/methodology for the future delivery of trainings, webinars and learning modules.

(3) **Reliable data**: The reports must be based on accurate and up-to-date data, coming from verified sources. Sources must always be indicated in the reports.

(4) **Sound analysis**: The analysis to be carried out for the performance of the different tasks (and in particular tasks 1 and 2) must rely on solid data and evidence. The methodology to achieve the analysis must be detailed and show how it will allow reaching valid conclusions in view of the objective of this Call.

(5) **Valid conclusions**: The conclusions must enable the Commission to have a clear understanding of the situation and the current challenges, exemplified by concrete examples. The conclusions must provide clear, actionable and concrete recommendations.

### 1.4.6 Deliverables

The contractor must provide the deliverables in accordance with the conditions of the draft service contract.

When requested in the contract the report(s) and deliverables will accompany the request(s) for payments.

Each report or document will be submitted in electronic format compatible with Microsoft Office (Word, Excel) and PDF or equivalent in English.

The contractor must ensure that all reports under the contract are drafted in professional/high-quality English using a clear, concise, understandable, user-friendly language.

Materials and deliverables for publication (online and/or printed) will be of the highest linguistic quality and will have been edited and proofread by a native speaker or equivalent. All reports should be consistent in style (headings, margins, citations, bibliography, etc.).

**It will remain contractor's responsibility to ensure a properly application of quotation and the verification of improper re-use of existing material.**
Technical Deliverables:

**Deliverables of Task 1 are:**

**Task 1.1:**
Introductory report defining the problem. The report must identify five target sectors and three use cases per sector.

**Task 1.2:**
A report providing a mapping of existing public awareness initiatives and instruments as well as recommendations for improvement.

**Task 1.3:**
Deliverables will include:
- A questionnaire;
- A fielding strategy: list of businesses to contact, timeline, refined fielding the strategy to achieve the minimum target number of responses;
- Raw results: Written summary of in-depth interviews;
- Quantitative and qualitative exhaustive descriptive statistics;
- A report on good practices, which must include an in-depth assessment based on the analysis of the results, concrete examples and use cases;
- Conclusions on means for businesses to effectively counter cyber-misappropriation of trade secrets in their daily operations.

**Deliverables of Task 2 are:**

**Research and training materials**

**Task 2.1:**
- Sectoral business guides;
- List of FAQs;
- Report on good practices;
- Report on additional tools proposed by the contractor, as indicated under Task 2.1.

**Task 2.2:**
- An integrated strategy/methodology for the future delivery of training modules
- Content of training modules.

**Task 2.3:**
- Testing of training modules.

**Task 2.4:**
- A detailed concept note for a web-portal

**Deliverables of Task 3 are:**

**Task 3.1**
- Strategy on the dissemination of the Toolkit;

**Tasks 3.1 and 3.2**
- A report including an outline of social media programs, an outline of KPIs to monitor the impact of awareness raising actions and policy recommendations.

**Deliverable of Task 4 is:**

- **Report on the event**

**Intermediate outputs and deliverables**

**Inception report**

The inception report must include a first definition of the problem to be further developed in the introductory report. The inception report must identify five target sectors and three use cases per sector.

**Progress reports**

At least three progress reports will be delivered. The first progress report must include deliverables under Task 1.1, Task 1.2, as well as the questionnaire and fielding strategy under deliverable 1.3. The second progress report must include a blueprint of deliverables under Tasks 2.1, 2.2, 2.4, 3.1 and 3.2. The third progress report must include the deliverables under Tasks 2.1 and 2.3.

The progress reports can be presented, for instance, in a form of a table containing the following information:

<table>
<thead>
<tr>
<th>Activities performed so far</th>
<th>Status and short description</th>
<th>Key next steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(examples)</em> Project management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meetings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>e.g. Task 1.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Interim Reports**

The contractor shall provide a first Interim Report in month 4 and 2 weeks of the contract implementation, which shall build on the structure agreed with in the inception report and form the basis for the Final Report. The first Interim Report will trigger an interim payment, as specified in the table in section 1.4.8 below. The first Interim Report will describe in detail what has been achieved in the reporting period and shall contain the list of pre-existing rights.

The first Interim Report must include deliverables under Task 1.1, Task 1.2, as well as the questionnaire, fielding strategy, the raw results and statistics under deliverable 1.3. This report must include a first draft of the report on good practices and conclusions under deliverable 1.3. The interim report will also include a plan for the organisation of the workshop.
The contractor shall provide a second Interim Report, in month 10 and 2 weeks of the contract implementation. The second Interim Report will describe in detail what has been achieved in the reporting period and shall also include a plan for the organisation of the testing of the pilot training modules.

**Final outputs and deliverables**

The final output and deliverables will include all technical deliverables related to Tasks 1 to 4, as listed above under section 1.4.6.1, and the Final report.

**Final report**

The final report shall include all final outputs and deliverables covering all deliverables (under Tasks 1 to 4), in English, and adapted following the review by the Commission and EISMEA and accommodating Commission and EISMEA’s comments and/or requests for improvement.

The Final Report shall contain an abstract of no more than 200 words and an executive summary with a least 1800 words and a maximum of six pages, in English.

**1.4.7 Meetings**

A kick-off meeting will take place (remotely or in person, in Brussels) within two weeks of the signature of the contract. The contractor will present to EISMEA and the European Commission the planning of activities and meetings. The contractor will clearly explain how it intends to gather the required information, if not yet in the possession of EISMEA/the Commission.

Progress meetings will be held regularly. To ensure smooth co-operation, meetings, video and audio conferences can be organised by the parties at the request of any of them and at any time during the implementation of the contract. EISMEA and the Commission shall be able at their own initiative to discuss any issue related to the project with any member of the team and with any sub-contractor.

The contractor shall produce the minutes of each meeting within 3 working days.

**1.4.8 Indicative timetable**

The tenderer shall propose in its offer a detailed work plan, which clearly indicates the sequences and timing of the work. It must take into consideration the following indicative timetable elements:

<table>
<thead>
<tr>
<th>Timetable (months/weeks/days)</th>
<th>Meetings</th>
<th>Actions/Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference date (T0)</td>
<td>Start date of the contract</td>
<td></td>
</tr>
<tr>
<td>T0 + 14 days</td>
<td>Kick-off meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 21 days</td>
<td>Inception report</td>
<td></td>
</tr>
<tr>
<td>T0 + 2 months 2 weeks</td>
<td>First progress report</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td>T0 + 3 months</td>
<td>First progress meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 4 months 2 weeks</td>
<td>First Interim Report Request for interim payment (40% of the total value of the contract).</td>
<td></td>
</tr>
<tr>
<td>T0 + 5 months</td>
<td>Interim meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 8 months 2 weeks</td>
<td>Second progress meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 9 months</td>
<td>Second progress meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 10 months 2 weeks</td>
<td>Second Interim Report</td>
<td></td>
</tr>
<tr>
<td>T0 + 11 months</td>
<td>Interim meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 14 months 2 weeks</td>
<td>Third progress report</td>
<td></td>
</tr>
<tr>
<td>T0 + 15 months</td>
<td>Third progress meeting</td>
<td></td>
</tr>
<tr>
<td>T0 + 16 months</td>
<td>Workshop</td>
<td></td>
</tr>
<tr>
<td>T0 + 17 months</td>
<td>Draft final report</td>
<td></td>
</tr>
<tr>
<td>T0 + 17 months 2 weeks</td>
<td>Final report</td>
<td></td>
</tr>
<tr>
<td>T0 + 18 months</td>
<td>Final meeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Request for balance payment</td>
<td></td>
</tr>
</tbody>
</table>

**1.5 Place of performance: where will the contract be performed?**

The services will be performed on-line or at different locations such as:

- the contractor's premises;
- other locations, such as Brussels or different locations for the implementation of the tasks described above.

**1.6 Nature of the contract: how will the contract be implemented?**

The procedure will result in the conclusion of a direct contract.

In direct contracts all the terms governing the provision of the services are defined at the outset. Once signed, they can be implemented directly without any further contract procedures.

† Tenderers need to take full account of the provisions of the Draft contract as the latter will define and govern the contractual relationship(s) to be established between the Contracting authority and the successful tenderer(s). Special attention is to be paid to the provisions specifying the rights and obligations of the contractor, in particular those on payments, performance of the contract, confidentiality, and checks and audits.
1.7 Volume and value of the contract: how much do we plan to buy?

The maximum amount of all purchases under this contract is indicated under Heading II.1.5 of the contract notice and is EUR 300 000, including all charges and expenses. No contract offer above this amount will be considered. The services to be purchased over the total duration of the contract are specified in Section 1.4 of these specifications.

1.8 Duration of the contract: how long do we plan to use the contract?

The contract resulting from the award of this call for tenders will be concluded for at most 18 months.

The execution of the tasks shall not start before the contract has been signed. Work will follow the timetable detailed in Section 1.4.8 of these specifications.

1.9 Electronic exchange system: can exchanges under the contract be automated?

For all exchanges with the contractor during the implementation of the contract as well as for future possible subsequent proceedings for the purposes of EDES (European Union's Early Detection and Exclusion System) the Contracting authority may use an electronic exchange system meeting the requirements of Article 148 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union. At the request of the Contracting authority the use of such a system shall become mandatory for the contractor at no additional cost for the Contracting authority. Details on specifications, access, terms and conditions of use will be provided in advance.
2 General information on tendering

2.1 Legal basis: what are the rules?

This call for tenders is governed by the provisions of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union (the Financial Regulation)\textsuperscript{42}.

The Contracting authority has chosen to award the contract resulting from this call for tenders through an open procedure pursuant to Article 164(1) (a) of the Financial Regulation. In an open procedure any interested economic operator (any natural or legal person who offers to supply products, provide services or execute works) may submit a tender.

The call for tenders is based on the Commission Implementing Decision C(2021) 3046 of 6 May 2021 on the financing of the Programme for Single Market, competitiveness of enterprises, including small and medium sized enterprises, and European Statistics and the Adoption of the Work Programme for 2021-2024 \textsuperscript{43}, Annex 2 Point 3.12, Supporting Actions \textsuperscript{44}.

2.2 Entities subject to restrictive measures and rules on access to procurement: who may submit a tender?

Participation in this call for tenders is open on equal terms to all natural and legal persons coming within the scope of the Treaties, as well as to international organisations.

It is also open to all natural and legal persons established in a third country, which has a special agreement with the European Union in the field of public procurement, such as the Stabilisation and Association Agreements (SAA) or the European Economic Area Agreement (EEA), on the conditions laid down in these agreements\textsuperscript{45}.


\textsuperscript{45} Third countries which have a special agreement with the European Union in the field of public procurement are:

- Under the Stabilisation and Association Agreements (SAA): North Macedonia, Albania, Montenegro, Bosnia and Herzegovina, Serbia, Kosovo;
- Under the European Economic Area (EEA) Agreement: Iceland, Norway and Liechtenstein.
States covered by the Agreement on Government Procurement con\ed within the World Trade Organisation are not included in this call for tenders as the Executive Agencies are not signatories of the Agreement.

For third countries participating in the Programme for Single Market, competitiveness of enterprises, including small and medium sized enterprises, and European Statistics:

Participation in this call for tenders is also open on equal terms to all natural and legal persons established in a third country eligible for funding under the Programme for Single Market, competitiveness of enterprises, including small and medium sized enterprises, and European Statistics.

Third countries negotiating association to the programme will be treated as associated countries provided that the association agreement with the third country concerned applies at the time of the award of the contract.

Tenderers must ensure that none of the involved entities (see Section 2.4) are subject to EU restrictive measures adopted under Article 29 of the Treaty on the European Union (TEU) or Article 215 of the Treaty on the Functioning of the EU (TFEU). The prohibition applies throughout the whole performance of the contract.

In case of a joint tender (see Section 2.4.1), each member of the group must have access to this procurement procedure.

The rules on access to procurement do not apply to subcontractors. Subcontracting may not be used with the intent to circumvent the rules on access to procurement.

To enable the Contracting authority to verify the access, each tenderer must indicate its country of establishment (and in case of joint tender – the country of establishment of each group member) in Annex 5 Letter of submission and must present the supporting evidence normally acceptable under the law of that country/ies. The same document(s) could be used to prove country/ies of establishment and the delegation(s) of the authorisation to sign as described in Section 4.3.

2.3 Registration in the Participant Register: why register?

Any economic operator willing to submit a tender for this call for tenders must be registered in the Participant Register - an online register of organisations and natural persons participating in European Commission's calls for tenders or proposals (participants).

---

46 https://www.wto.org/english/tratop_E/gproc_e/gp_gpa_e.htm
49 Please note that the EU Official Journal contains the official list of entities subject to restrictive measures and, in case of conflict, it prevails over the list of the EU Sanctions Map.
50 The supporting evidence are to be provided when requested by the EU Validation Services
On registering each participant obtains a Participant Identification Code (PIC, 9-digit number) which acts as its unique identifier in the Participant Register. A participant needs to register only once – the information provided can be further updated or re-used by the participant in other EISMEA’s and European Commission's calls for tenders or calls for proposals.

**Please provide information about the SME status of the participant in the Participant Register by filling in the SME Declaration section in the Participant Register. The section becomes available only when updating/modifying the details of the registered organisation.**

At any moment during the procurement procedure the Research Executive Agency Validation Services (hereafter the EU Validation Services) may contact the participant and ask for supporting documents on legal existence, status and financial capacity. The requests will be made through the register's messaging system to the e-mail address of the participant's contact person indicated in the register. It is the responsibility of the participant to provide a valid e-mail address and to check it regularly.

The documents that may be requested by the EU Validation Services are listed in the EU Grants and Tenders Rules on Legal Entity Validation, LEAR appointment and Financial Capacity assessment.

**Please note that a request for supporting documents by the EU Validation Services in no way implies that the tenderer has been successful.**

### 2.4 Ways to submit a tender: how can economic operators organise themselves to submit a tender?

Economic operators can submit a tender either as a sole economic operator (sole tenderer) or as a group of economic operators (joint tenderer). In either case, subcontracting is permitted.

In order to fulfil the selection criteria set out in Section 3.2 the tenderer can rely on the capacities of subcontractors or other entities that are not subcontractors.

The role of each entity involved in a tender (hereafter referred to as “involved entity”) must be clearly specified in the eSubmission application: i) sole tenderer, ii) Group leader of group of tenders, iii) member of a group of tenderers, or iv) subcontractor. For an entity on whose capacities the tenderer relies to fulfil the selection criteria (that is not a subcontractor), this role is defined in the commitment letter (Annex 5.2). This applies also where the involved entities belong to the same economic group (see Section 2.4.3).

---

51 Such an entity is not considered a subcontractor, see Section 2.4.3.
2.4.1 Joint tenders

A joint tender is a situation where a tender is submitted by a group (with or without legal form) of economic operators regardless of the link they have between them. The group as a whole is considered a tenderer\textsuperscript{52}.

All members of the group assume joint and several liability towards the Contracting authority for the performance of the contract as a whole.

Group members must appoint a Group leader and a single point of contact authorised to act on their behalf in connection with the submission of the tender and all relevant questions, clarification requests, notifications, etc., that may be received during the evaluation, award and until the contract signature. The model power of attorney attached in Annex 3 is to be used.

The joint tender must clearly indicate the role and tasks of each member and of the Group leader who will act as the Contracting authority's contact point for the contract's administrative or financial aspects and operational management. The Group leader will have full authority to bind the group and each of its members during contract execution. If the joint tender is successful, the Contracting authority shall sign the contract with the Group leader, authorised by the other members to sign the contract on their behalf via power of attorney drawn up in Annex 3.

Changes in the composition of the group during the procurement procedure (after the submission deadline and before contract signature) shall lead to rejection of the tender except in case of a merger or takeover of a member of the group (universal succession), provided that the new entity has access to procurement (see Section 2.2), and is not in an exclusion situation. (see Section 3.1)

In any case the selection criteria must be still fulfilled by the group and the terms of the originally submitted tender may not be altered substantially, i.e. all the tasks assigned to the former entity must be taken over by the new entity member of the group, the change must not make the tender non-compliant with the Tender specifications, and the evaluation of award criteria of the originally submitted tender may not be modified.

2.4.2 Subcontracting

Subcontracting is the situation where the contractor enters into legal commitments with other economic operators, which will perform part of the contract on its behalf. The contractor retains full liability towards the Contracting authority for performance of the contract as a whole.

The following shall not be considered subcontracting:

a) Use of workers posted to the contractor by another company owned by the same group and established in a Member State (“intra-group posting” as defined by Article 1, 3, (b) of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services).

\textsuperscript{52} References to tenderer or tenderers in this document shall be understood as covering both sole tenderers and groups of economic operators submitting a joint tender.
b) Use of workers hired out to the contractor by a temporary employment undertaking established in a Member State ("hiring out of workers" as defined by Article 1, 3, (c) of Directive 96/71/EC concerning the posting of workers in the framework of the provision of services).

c) Use of workers temporarily transferred to the contractor from an undertaking established outside the territory of a Member State and that belongs to the same group ("intra-corporate transfer" as defined by Article 3, (b) of Directive 2014/66/EU on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer).

d) Use of staff without employment contract ("self-employed persons working for the contractor"), without the tasks of the self-employed persons being particular well-defined parts of the contract.

e) Use of suppliers and/or transporters by the contractor, in order to perform the contract at the place of performance, unless the economic activities of the suppliers and/or the transporting services are within the subject of this call for tenders (see Section 1.4).

f) Performance of part of the contract by members of an EEIG (European Economic Interest Grouping), when the EEIG is itself a contractor or a group member.

The persons mentioned in points a, b, c and d above will be considered as "personnel" of the contractor as defined in the contract.

All contractual tasks may be subcontracted unless the Technical specifications expressly reserve the execution of certain critical tasks to the sole tenderer itself, or in case of a joint tender, to a member of the group.

By filling in the form available in Annex 4 List of Subcontractors, tenderers are required to:

i. give an indication of the proportion of the contract that they intend to subcontract, as well as to identify and describe briefly the envisaged contractual roles/tasks of subcontractors meeting any of these conditions (hereafter referred to as identified subcontractors):

- on whose capacities the tenderer relies upon to fulfil the selection criteria as described under Section 3.2;

- whose individual share of the contract, known at the time of submission, is above 10%.

Any such identified subcontractor must provide the tenderer with a commitment letter drawn up in the model attached in Annex 5.1 and signed by its authorised representative.

ii. list all other subcontractors who do not meet any of the conditions above. Those subcontractors are not requested to provide a commitment letter.

Changes concerning subcontractors identified in the tender (withdrawal/replacement of a subcontractor, additional subcontracting) during the procurement procedure (after the
submission deadline and before contract signature) require the prior written approval of the Contracting authority subject to the following verifications:

- any new subcontractor is not in an exclusion situation;
- the tenderer still fulfils the selection criteria and the new subcontractor fulfils the selection criteria applicable to it individually, if any;
- the terms of the originally submitted tender are not altered substantially, i.e. all the tasks assigned to the former subcontractor are taken over by another involved entity, the change does not make the tender non-compliant with the Tender specifications, and the evaluation of award criteria of the originally submitted tender is not modified.

Subcontracting to subcontractors identified in a tender that was accepted by the Contracting authority and resulted in a signed contract, is considered authorised.

2.4.3 Entities on whose capacities the tenderer relies to fulfil the selection criteria

In order to fulfil the selection criteria a tenderer may also rely on the capacities of other entities, regardless of the legal nature of the links it has with them. It must in that case prove that it will have at its disposal the resources necessary for the performance of the contract by producing a commitment letter in the model attached in Annex 5.2, signed by the authorised representative of such an entity, and the supporting evidence that those other entities have the respective resources.

If the contract is awarded to a tenderer intending to rely on another entity to meet the minimum levels of economic and financial capacity, the Contracting authority may require the entity to sign the contract or, alternatively, to provide a joint and several first-call financial guarantee for the performance of the contract.

With regard to technical and professional selection criteria, a tenderer may only rely on the capacities of other entities where the latter will perform the works or services for which these capacities are required.

† Relying on the capacities of other entities is only necessary when the capacity of the tenderer is not sufficient to fulfil the required minimum levels of capacity. Abstract commitments that other entities will put resources at the disposal of the tenderer will be disregarded.
3 Evaluation and award

The evaluation of the tenders that comply with the submission conditions will consist of the following elements:

- Check if the tenderer has access to procurement Annex 5 Letter of Submission;
- Verification of administrative compliance (if the tender is drawn up in one of the official EU languages and the required documents Annex 5 Letter of Submission and Annex 3 Power of Attorney signed by duly authorised representative(-s) of the tenderer);
- Verification of non-exclusion of tenderers on the basis of the exclusion criteria;
- Selection of tenderers on the basis of selection criteria;
- Verification of compliance with the minimum requirements specified in the procurement documents;
- Evaluation of tenders on the basis of the award criteria.

The Contracting authority will evaluate the abovementioned elements in the order that it considers to be the most appropriate. If the evaluation of one or more elements demonstrates that there are grounds for rejection, the tender will be rejected and will not be subjected to further full evaluation. The unsuccessful tenderers will be informed of the ground for rejection without being given feedback on the non-assessed content of their tenders. Only tenderer(s) for whom the verification of all elements did not reveal grounds for rejection can be awarded the contract.

The evaluation will be based on the information and evidence contained in the tenders and, if applicable, on additional information and evidence provided at the request of the Contracting authority during the procedure. If any of the declarations or information provided proves to be false, the Contracting authority may impose administrative sanctions (exclusion or financial penalties) on the entity providing the false declarations/information.

For the purposes of the evaluation related to exclusion and selection criteria the Contracting authority may also refer to publicly available information, in particular evidence that it can access on a national database free of charge.

3.1 Exclusion criteria

The objective of the exclusion criteria is to assess whether the tenderer is in any of the exclusion situations listed in Article 136(1) of the Financial Regulation.

Tenderers found to be in an exclusion situation will be rejected.
As evidence of non-exclusion each tenderer needs to submit with its tender a Declaration on Honour in the model available in Annex 2. The declaration must be signed by an authorised representative of the entity providing the declaration.

The initial verification of non-exclusion of tenderers will be done on the basis of the submitted declarations and consultation of the European Union's Early Detection and Exclusion System. The documents mentioned as supporting evidence in the Declaration on Honour need to be provided whenever requested and where this is necessary to ensure the proper conduct of the procedure within a deadline given by the Contracting authority.

Annex 1 specifies which of the involved entities participating in a tender need to provide the Declaration on Honour and, when requested by the Contracting authority, the supporting evidence.

Before the award decision, the contracting authority may request documentary evidence on compliance on the exclusion criteria set out in the present tender specifications. All tenderers are invited to prepare in advance the documents related to the evidence, since they may be requested to provide such evidence within a short deadline. Failure to provide valid documentary evidence within the deadline set by the Contracting Authority shall lead to the rejection of the tender for the award of the contract, unless the tenderer can justify the failure on the grounds of material impossibility.

Please note that a request for evidence in no way implies that the tenderer has been successful.

3.2 Selection criteria

The objective of the selection criteria is to assess whether the tenderer has the economic, financial, technical and professional capacity to perform the contract.

The selection criteria for this call for tenders, including the minimum levels of capacity, the basis for assessment and the evidence required, are specified in the following subsections.

53 The European Single Procurement Document (ESPD) may not be used yet in the Contracting authority’s calls for tenders.
54 Unless the same declaration has already been submitted for the purposes of another award procedure of the Contracting authority, the situation has not changed, and the time elapsed since the issuing date of the declaration does not exceed one year.
55 The obligation to provide the supporting evidence will be waived in the following situations:
- if the same documents have already been provided in a previous award procedure of the same Contracting authority, have been issued no more than one year before the date of their request by the Contracting authority and are still valid at that date;
- if such evidence can be accessed by the Contracting authority on a national database free of charge, in which case the economic operator shall provide the Contracting authority with the internet address of the database and, if needed, the necessary identification data to retrieve the document;
- if there is a material impossibility to provide such evidence.
Tenders submitted by tenderers not meeting the minimum levels of capacity will be rejected.

When submitting its tender each tenderer shall declare on honour that it fulfils the selection criteria for the call for tender. The model Declaration on Honour available in Annex 2 shall be used.

The initial assessment of whether a tenderer fulfils the selection criteria will be done on the basis of the submitted declaration(s) and the information included in the tables in Annex 2.1 Statement on turnover and Annex 2.2 Technical capacity fully completed and the evidence where requested.

The subsections below specify which selection criteria evidence must be provided with the tender or may be requested later, at any time during the procurement procedure. In any case, to the extent that there is no ground for a waiver, the evidence must be provided, upon request and within a deadline given by the Contracting authority. The evidence must be provided in accordance with the applicable basis for assessment of each criterion: in case of a consolidated assessment – only by the involved entities who contribute to the fulfilment of the criterion, and in case of individual assessment – by each involved entity to whom the criterion applies individually.

Before the award decision, the contracting authority may request documentary evidence on compliance with the selection criteria set out in the present tender specifications. All tenderers are invited to prepare in advance the documents related to the evidence, since they may be requested to provide such evidence in a short deadline. In any event, the tenderer proposed by the evaluation committee for the award of the contract, will be requested to provide such evidence.

Failure to provide valid documentary evidence within the deadline set by the Contracting Authority shall lead to the rejection of the tender for the award of the contract, unless the tenderer can justify the failure on the grounds of material impossibility.

3.2.1 Legal and regulatory capacity

Tenderers do not need to prove specific legal and regulatory capacity to perform the contract.

3.2.2 Economic and financial capacity

Tenderers must comply with the following selection criteria in order to prove that they have the necessary economic and financial capacity to perform the contract.

56 The obligation to provide the supporting evidence will be waived in the following situations:

- if the same documents have already been provided in a previous award procedure of the same Contracting authority and are still valid at that date;
- if such evidence can be accessed by the Contracting Authority on a national database free of charge, in which case the economic operator shall provide the Contracting authority with the internet address of the database and, if needed, the necessary identification data to retrieve the document.
<table>
<thead>
<tr>
<th><strong>Criterion F1</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum level of capacity</strong></td>
</tr>
<tr>
<td><strong>Basis for assessment</strong></td>
</tr>
<tr>
<td><strong>Evidence</strong></td>
</tr>
</tbody>
</table>

† Tenderers, including partners in a joint tender, and subcontractors must provide a Statement of Turnover in accordance with Annex 2.1 of these tender specifications completed with the information requested.

† The evidence of economic and financial capacity of the members of the group or sole tenderer does need not be provided with the tender but may be requested by the Contracting authority or the EU Validation Services at any time during the procedure.

† Only subcontractors contributing to the combined financial and economic capacity of tenderers should submit with the tender the following documents in eSubmission:

  ✓ Copy of the Profit and Loss accounts for the last two years for which the accounts have been closed from each concerned legal entity;

  Failing that,

  ✓ Appropriate statements from banks;

  Or,

  Evidence of professional risk indemnity insurance.

Please note that a request for evidence in no way implies that the tenderer has been successful.
3.2.3 Technical and professional capacity

Tenderers must comply with the following selection criteria in order to prove that they have the necessary technical capacity to perform the contract.

Tenders must provide in their tender the table in Annex 2.2 of these tender specifications, exhaustively completed with all the necessary information.

A. Criteria relating to tenderers:

<table>
<thead>
<tr>
<th>Criterion T1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The tenderer must prove experience in the field of cyber security.</strong></td>
</tr>
<tr>
<td><strong>Minimum level of capacity</strong></td>
</tr>
<tr>
<td><strong>Basis for assessment</strong></td>
</tr>
<tr>
<td><strong>Evidence</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criterion T2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The tenderer must prove experience in the field of trade secrets and intellectual property management advice to companies.</strong></td>
</tr>
<tr>
<td><strong>Minimum level of capacity</strong></td>
</tr>
<tr>
<td><strong>Basis for assessment</strong></td>
</tr>
<tr>
<td><strong>Evidence</strong></td>
</tr>
</tbody>
</table>
The tenderer must prove experience in the field of survey techniques, data collection and analysis.

**Criterion T3**

**Minimum level of capacity**
At least 2 projects showing experience in data collection and analysis (e.g. organisation of interviews, surveys, analysis of data, etc.), completed in the last 4 years preceding the tender submission deadline, with a minimum value for each of them EUR 100,000.

**Basis for assessment**
This criterion applies to the tenderer as a whole, i.e. the combined capacities of all involved entities (all members of the group and identified subcontractors).

**Evidence**
A list of projects meeting the minimum level of capacity. The list shall include details of their title and main activities, start and end date, total project amount, role of implementing entity (leader, partner, subcontractor, etc.) and amount invoiced. In case of projects still on-going only the portion completed during the reference period will be taken into consideration.

As supporting documents for each project reference the Contracting authority may request statements issued by the clients and take contact with them.

The tenderer must prove experience in the field of preparation, dissemination of awareness raising tools and stakeholders outreach.

**Criterion T4**

**Minimum level of capacity**
At least 2 projects showing experience in preparing awareness raising and training tools (e.g. guides, FAQs, etc.), in the dissemination of awareness raising material (e.g. trainings, workshops, etc.) and stakeholders outreach completed in the last 4 years preceding the tender submission deadline, with a minimum value for each of them EUR 50,000.

**Basis for assessment**
This criterion applies to the tenderer as a whole, i.e. the combined capacities of all involved entities (all members of the group and identified subcontractors).

**Evidence**
A list of projects meeting the minimum level of capacity. The list shall include details of their start and end date, total project amount and scope, role and
amount invoiced. In case of projects still on-going only the portion completed during the reference period will be taken into consideration.

As supporting documents for each project reference the Contracting authority may request statements issued by the clients and take contact with them.

Involved entities must not be subject to conflicting interests, which may negatively affect the contract performance. Where the Contracting authority has established such conflicting interests, it may conclude that the tenderer or an involved entity does not possess the required professional capacity to perform the contract to an appropriate quality standard.

The presence of conflicting interests shall be examined during the evaluation phase based on the statements made through the Annex 2 Declaration on Honour and, where applicable, the commitment letters (Annex 5.1 and Annex 5.2).

B. Criteria relating to the team delivering the service:

Tenderers must comply with the following selection criteria in order to prove that they have the necessary professional capacity to perform the contract.

The team delivering the service shall be assessed for the tenderer as a whole, i.e. the team members can be proposed by all involved entities (including partners and subcontractors). The team should include, as a minimum, the following profiles.

Evidence will consist in CVs in EUROPASS format of the team responsible to deliver the service. Each CV should indicate the intended function in the delivery of the service.

A detailed CV in the EUROPASS format must specify:

- Educational and professional qualifications and experience in areas relevant to the subject of these tender specifications;
- Different diplomas or degrees obtained;
- Level of the languages spoken.

The contractor shall ensure that the staff members listed in the technical offer are effectively available when the contract begins.
### Criterion P1

**Project manager**

**Minimum level of capacity**

At least ten years’ experience in project management, including overseeing project delivery, quality control of delivered service, client orientation and conflict resolution experience in a project of at least €200,000 and geographical coverage of at least 10 countries, with experience in management of a team of at least 10 people.

The project manager shall be fluent in English (at least C1 level in the European Framework of Reference for Languages\(^{57}\)).

**Basis for assessment**

This criterion applies to the individual foreseen for this position.

**Evidence**

CV with a list of relevant projects managed and a language certificate or past relevant experience or mother tongue.

As supporting documents, the Contracting authority may request a document proving the qualifications (copy of diploma, etc.).

### Criterion P2

**Experts in the following areas: 1) trade secret protection, 2) cybersecurity, 3) data collection and analysis techniques**

**Minimum level of capacity**

At least one expert per area: 1) trade secret protection, 2) cybersecurity, 3) data collection and analysis techniques.

For each of the experts:

At least 5 years of professional experience in the respective area and higher education (Bachelor or Master) degree in Information Technology, business, law, digital studies, studies in cybersecurity issues or equivalent.

**Basis for assessment**

This criterion applies to the individuals proposed.

**Evidence**

CV showing the specific experience and the educational qualifications.

As supporting documents, the Contracting authority may request a document proving the qualifications (copy of diploma, etc.).

---

may request a document proving the qualifications (copy of diploma, etc.).

**Criterion P3**

**Experts in designing, testing, and delivering online courses and events, as well as organising online learning resources, through an online platform**

| **Minimum level of capacity** | At least two experts in designing, testing and delivering online courses and events, as well as organising online learning resources, through an online platform. At least 3 years of professional experience, and higher education degree in education studies, pedagogy, digital studies, information and communications technology studies or communication. |
| **Basis for assessment** | This criterion applies to the individuals proposed. |
| **Evidence** | CV showing the specific experience and the educational qualifications.  
As supporting documents, the Contracting authority may request a document proving the qualifications (copy of diploma, etc.). |

**Criterion P4**

**Expert in advising businesses on legal aspects of trade secrets and confidential business information**

| **Minimum level of capacity** | At least one expert with at least 7 years of professional experience in advising businesses on legal aspects of trade secrets and confidential business information and higher education degree in law, or equivalent. |
| **Basis for assessment** | This criterion applies to the individuals proposed. |
| **Evidence** | CV showing the specific experience and the educational qualifications.  
As supporting documents, the Contracting authority may request a document proving the qualifications (copy of diploma, etc.). |

**Criterion P5**

**Members of the team fluent in English language**
### Minimum level of capacity

All members of the team shall have a level of English that is native-level or C1 level in the Common European Framework of Reference for Languages\(^{58}\).

### Basis for assessment

This criterion applies to the individuals proposed.

### Evidence

CV with a language certificate or past relevant experience or mother tongue.

---

**Criterion P6**

**Expert on communication and dissemination (social media)**

<table>
<thead>
<tr>
<th>Minimum level of capacity</th>
<th>At least 2 experts with each at least 4 years of professional experience in communication and dissemination, with a special focus on social media.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis for assessment</td>
<td>This criterion applies to the individuals proposed.</td>
</tr>
<tr>
<td>Evidence</td>
<td>CV with a language certificate or past relevant experience or mother tongue.</td>
</tr>
<tr>
<td></td>
<td>As supporting documents, the Contracting authority may request a document proving the qualifications (copy of diploma, etc.).</td>
</tr>
</tbody>
</table>

\(^{58}\) Only CVs must be provided with the tender. The other evidence of technical and professional capacity may be requested by the Contracting authority at any time during the procedure. **Please note that a request for evidence in no way implies that the tenderer has been successful.**

---

### 3.3 Compliance with the minimum requirements of the procurement documents

By submitting a tender a tenderer commits to perform the contract in full compliance with the terms and conditions of the procurement documents for this call for tenders.

Particular attention is drawn to the minimum requirements specified in **Section 1.4** of these specifications and to the fact that tenders must comply with applicable data protection, environmental, social and labour law obligations established by Union law, national legislation, collective agreements or the international environmental, social and labour conventions listed in Annex X to Directive 2014/24/EU.

---

Information about the environmental policy of EISMEA is provided in annex to these specifications.

The minimum requirements shall be observed throughout the entire duration of the contract. Compliance with these requirements is mandatory and cannot be subject to any assumptions, limitations, conditions, or reservations on the part of a tenderer.

Tenders that are not compliant with the applicable minimum requirements shall be rejected.

### 3.4 Award criteria

The objective of the award criteria is to evaluate the tenders with a view to choosing the most economically advantageous tender.

Tenders will be evaluated on the basis of the following award criteria and their weighting:

<table>
<thead>
<tr>
<th>Quality</th>
<th>award criterion</th>
<th>Explanation of the criterion’s scope</th>
<th>Maximum number of points per criterion (out of 100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price</td>
<td>1. Price - 30 %</td>
<td>The price considered for evaluation will be the total price of the tender, quoted under &quot;A - Total price of the contract and total price used for the assessment of the financial offer&quot; (as per Annex 6 Price and breakdown of prices (Financial offer form) covering all the requirements set out in the Tender specifications.)</td>
<td>50</td>
</tr>
<tr>
<td>Quality</td>
<td>2. Quality - 70 %</td>
<td>The quality of the tender will be evaluated based on the following criteria:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quality, appropriateness and completeness of the proposed methodology to complete the tasks</td>
<td>This criterion will evaluate, inter alia: - the quality and clarity of the information for a sufficient identification of and access to sources of information (research and mapping) - the coherency and completeness of the strategy for data collections and analysis; and coherency, quality and adequacy of organisation and the exploitation of surveys and interview; - the adequacy and clarity of methodology for the setting-up of guides, FAQs, trainings, learning</td>
<td>50</td>
</tr>
</tbody>
</table>
- the adequacy and clarity of methodology as to the organisation and dissemination of the awareness raising material in a business-friendly, jargon-free way;
- the comprehensiveness of methodology as to the formulation of relevant conclusions and recommendations.

**Impact**

This criterion will assess the following issues:

- inclusiveness of relevant institutions involved in developing the concept, design
- inclusiveness and approach to the selection of best practices
- the approach and inclusiveness of the process regarding the development of toolkit;
- demonstration of potential for sustainability, replicability and continuous development of the training programme
- visibility of the European dimension and added value of the toolkit and recommendations, and of the European Commission’s contribution to supporting companies against cyber theft.

**Organisation of the work and resources**

This criterion will assess how the roles and responsibilities of the proposed team and of the different economic operators (in case of joint tenders, including subcontractors if applicable) are distributed for each task. It also assesses the global allocation of time and resources to the project and to each task or deliverable, and whether this allocation is adequate for the work.

The tender should provide details on the allocation of time and human resources and the rationale behind the choice of this allocation. Details should be provided as part of the technical offer. Units costs/prices are to be included in the financial offer only.
**Quality control measures**

This criterion will assess the quality control system applied to the service foreseen in this tender specification concerning the quality of the deliverables, the language quality check, and continuity of the service in case of absence of the member of the team. The quality system should be detailed in the tender and specific to the tasks at hand.

Generic quality system will result in a low score.

<table>
<thead>
<tr>
<th>Strategy for a reduced environmental impact of tasks and deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategies and methods proposed to ensure proper respect of environmental considerations, the limitation of environmental impact of services carried out, organisation of low emissions events, waste prevention and recycling.</td>
</tr>
</tbody>
</table>

| Total | 100 |

The result of the technical evaluation is the sum of the points obtained based on the evaluation of each criterion (maximum 100 points).

Only those tenders that score:

- at least 50% for each criterion and
- at least 70% of the total points will be considered for the award of the contract.

Tenders not reaching the minimum quality threshold will not be further assessed. Their financial tenders will therefore not be considered for determining the cheapest reference price.

### 3.5 Award (ranking of tenders)

Tenders shall be ranked according to the best price-quality ratio in accordance with the formula below:

\[
\text{score for tender X} = \frac{\text{cheapest reference price}}{\text{reference price of tender X}} \times 100 \times \text{price weighting (30%)} + \text{total quality score for all award criteria of tender X} \times \text{quality weighting (70%)}
\]

Should the outcome of the formula lead to two or more tenders with the same result, the tenderer who has been awarded the highest marks for quality will be deemed to be the
most economically advantageous tender. This approach will continue to be applied to each of the award criteria in the descending order listed in below until a most economically advantageous tender can be determined:

1. Quality, appropriateness and completeness of the proposed methodology to complete the tasks;

2. Impact;

3. Organisation of work and resources;

4. Quality control measures;

5. Strategy for a reduced environmental impact of tasks and deliverables.

The contract shall be awarded to the tender ranked first, which complies with the Tender Specifications and is submitted by a tenderer having access to procurement, not in an exclusion situation and fulfilling with the selection criteria.
4 Form and content of the tender

4.1 Form of the tender: how to submit the tender?

Tenders are to be submitted via the eSubmission application according to the instructions laid down in the Invitation to tender letter and the eSubmission Quick Guide.

Make sure you prepare and submit your electronic tender in eSubmission early enough to ensure it is received within the deadline specified under Heading IV.2.2 of the contract notice.

4.2 Content of the tender: what documents to submit with the tender?

The documents to be submitted with the tender in eSubmission are listed in Annex 1.

The following requirements apply to the technical and financial offer (to be uploaded as eSubmission):

- **Technical offer**

  The technical offer must provide all the information needed to assess the compliance with Section 1.4 of these specifications and the award criteria. Tenders deviating from the minimum requirements or not covering all the requirements may be rejected on the basis of non-compliance and not evaluated further.

  For the appraisal, the written submission shall include a clear and detailed description of the organisation, resources and methodology proposed. Tenderers will provide a practical and detailed description of the resources and services proposed to achieve the objectives and results set out in Section 1.4 above. Tenderers will also provide a summary of their technical offer in Annex 7 Technical tender form.

  The tender should provide details on the allocation of time and human resources and the rationale behind the choice of this allocation. Details should be provided as part of the technical offer, i.e. the allocation should be indicated for each tasks and should specify the role, the names and the estimated number of days/units for each member of the team. The balance between the efforts devoted to each task should be reasonable and well justified. This is not a request for a budget, as the budget should only be part of the financial offer.

  Tenderers are strongly advised to present their tenders (technical part) on maximum 50 pages, whereas CVs and other reference documents can be annexed, which will not count towards the above-mentioned maximum. The technical offer must have all the
The Tenderers should be aware that if an offer significantly overpasses the advised maximum of 50 pages and this does not provide added value, the offer is not sufficiently focused, or does not contain information that is pertinent to the technical specification requirements, the evaluation of such offer will result in a lower score.

- **Financial offer**

A complete financial offer, including the breakdown of the price needs to be uploaded. For this purpose, the Financial offer form in *Annex 6* shall be completed, duly signed and uploaded in eSubmission. The total amount of the offer as indicated in cell <G113> must be encoded in the field “Total amount excl. taxes” under the section “Tender data” in eSubmission.

It is the responsibility of each tenderer to ensure that the total amount of the tender inserted in the relevant field “Total amount excl. taxes” corresponds to the amount indicated in the uploaded financial offer. In case of discrepancies, only the amount indicated in the financial offer will be taken into account.

The financial offer shall be:

- expressed in euros. Tenderers from countries outside the euro zone have to quote their prices in euro. The price quoted may not be revised in line with exchange rate movements. It is for the tenderer to bear the risks or the benefits deriving from any variation.

- quoted free of all duties, taxes and other charges, i.e. also free of VAT.

The quoted price must be a fixed amount which includes all charges (including travel and subsistence). Travel and subsistence expenses are not refundable separately.

Tenderers are also requested to explicitly indicate in the financial offer the efforts in terms of human resources corresponding to fees and prices, where applicable.

*The European Union Institutions are exempt from such charges in the EU under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union of 8 April 1965 annexed to the Treaty on the Functioning of the European Union. Exemption is granted to the Commission by the governments of the Member States, either through refunds upon presentation of documentary evidence or by direct exemption.*

In case of doubt about the applicable VAT system, it is the tenderer's responsibility to contact his or her national authorities to clarify the way in which the European Union is exempt from VAT.
4.3 Signature policy: how can documents be signed?

Where a document needs to be signed, the signature must be either hand-written, or a qualified electronic signature as defined in Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation).

For hand-written signatures see Section 1 of the Invitation to tender.

For electronic signatures see: https://webgate.ec.europa.eu/fpfis/wikis/x/YIrgIw

All documents must be signed by the signatories (when they are individuals) or by their duly authorised representatives.

For the following documents, when signed by representatives, tenderers must provide evidence for the delegation of the authorisation to sign:

- The Declaration on Honour (Annex 2) of the tenderer (in case of joint tender – the Declarations on Honour of all group members);
- (If applicable – in the case of joint tender) the power(s) of attorney drawn up using the model attached in Annex 3).
- The Letter of Submission (Annex 5)
- The Statement of turnover (Annex 2.1)

The delegation of the authorisation to sign on behalf of the signatories (including, in the case of proxy(-ies), the chain of authorisations) must be evidenced by appropriate written evidence (copy of the notice of appointment of the persons authorised to represent the legal entity in signing contracts (together or alone), or a copy of the publication of such appointment if the legislation which applies to signatory requires such publication or a power of attorney).

A document that the Contracting authority can access on a national database free of charge does not need to be submitted if the Contracting authority is provided with the exact internet link and, if applicable, the necessary identification data to retrieve the document.

4.4 Confidentiality of tenders: what information and under what conditions can be disclosed?

Once the Contracting authority has opened a tender, it becomes its property and shall be treated confidentially, subject to the following:

- For the purposes of evaluating the tender and, if applicable, implementing the contract, performing audits, benchmarking, etc., the Contracting authority is entitled to make available (any part of) the tender to its staff and the staff of other Union institutions, agencies and bodies, as well to other persons and entities working for the Contracting authority or cooperating with it, including
contractors or subcontractors and their staff provided that they are bound by an obligation of confidentiality.

- After the signature of the award decision tenderers whose tenders were received in accordance with the submission modalities, who have access to procurement, who are not found to be in an exclusion situation referred to in Article 136(1) of the FR, who are not rejected under Article 141 of the FR, whose tenders are not found to be incompliant with the procurement documents, and who make a request in writing will be notified of the name of the tenderer to whom the contract is awarded, the characteristics and relative advantages of the successful tenderer and the price of the offer and/or contract value. The Contracting authority may decide to withhold certain information that it assesses as being confidential, in particular where its release would prejudice the legitimate commercial interests of economic operators or might distort fair competition between them. Such information may include, without being limited to, confidential aspects of tenders such as unit prices included in the financial offer, technical or trade secrets.

- The Contracting authority may disclose the submitted tender in the context of a request for public access to documents, or in other cases where the applicable law requires its disclosure. Unless there is an overriding public interest in disclosure, the Contracting authority may refuse to provide full access to the submitted tender, redacting the parts (if any) that contain confidential information, the disclosure of which would undermine the protection of commercial interests of the tenderer, including intellectual property.

The Contracting authority will disregard general statements that the whole tender or substantial parts of it contain confidential information. Tenderers need to mark clearly the information they consider confidential and explain why it may not be disclosed. The Contracting authority reserves the right to make its own assessment of the confidential nature of any information contained in the tender.

---

59 For the definition of trade secrets please see Article 2 (1) of DIRECTIVE (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

60 See Article 4 (2) of the REGULATION (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents.
## 5 Appendix: List of references

<table>
<thead>
<tr>
<th>Award criteria</th>
<th>See Section 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contracting authority</td>
<td>See Section 1.1</td>
</tr>
<tr>
<td>Entities on whose capacities the tenderer relies to fulfil the selection criteria</td>
<td>See Section 2.4.3</td>
</tr>
<tr>
<td>EU Validation services</td>
<td>See Section 2.3</td>
</tr>
<tr>
<td>Exclusion criteria</td>
<td>See Section 0</td>
</tr>
<tr>
<td>Group leader</td>
<td>See Section 2.4.1</td>
</tr>
<tr>
<td>Identified subcontractors</td>
<td>See Section 2.4.2</td>
</tr>
<tr>
<td>Involved entities</td>
<td>See Section 2.4</td>
</tr>
<tr>
<td>Joint tender</td>
<td>See Section 2.4.1</td>
</tr>
<tr>
<td>Participating entities</td>
<td>See Section 1.1</td>
</tr>
<tr>
<td>Participant Register</td>
<td>See Section 2.3</td>
</tr>
<tr>
<td>Selection criteria</td>
<td>See Section 3.2</td>
</tr>
<tr>
<td>Sole tenderer</td>
<td>See Section 2.4</td>
</tr>
<tr>
<td>Subcontracting/subcontractor</td>
<td>See Section 2.4.2</td>
</tr>
<tr>
<td>Treaties</td>
<td>The EU Treaties:</td>
</tr>
</tbody>
</table>
6 Annexes

Annex 1 - List of documents to be submitted with the tender or during the procedure

Annex 2 - Declaration on honour on exclusion and selection criteria

Annex 2.1 – Statement of turnover

Annex 2.2 – Technical capacity

Annex 3 - Power of attorney

Annex 4 – List of subcontractors

Annex 5 – Letter of submission

Annex 5.1 - Commitment letter by an identified subcontractor

Annex 5.2 - Commitment letter by an entity on whose capacities is being relied

Annex 6 - Financial offer form

Annex 7 – Technical tender form

EISMEA Environmental policy

Draft service contract and Annexes