

TENDER SPECIFICATIONS

European Capability for Situational Awareness

SMART 2013/N004

PART 1: TECHNICAL DESCRIPTION	3
1 CONTEXT	3
2 OBJECTIVES	7
3 DURATION	15
4 DELIVERABLES, MEETINGS AND TIMETABLE	15
4.1.1 <i>The deliverables listed below must be provided by the contractor:</i>	15
4.1.2 <i>Report format</i>	16
4.1.3 <i>Content</i>	17
4.1.3.1 <i>Final Study Report</i>	17
4.1.3.2 <i>Publishable executive summary</i>	17
4.1.3.3 <i>Abstract</i>	18
4.1.4 <i>Structure</i>	18
4.1.5 <i>Graphic requirements</i>	19
4.2 <i>Meetings and workshops</i>	19
4.3 <i>Timetable</i>	21
5 TERMS OF APPROVAL OF REPORTS/DELIVERABLES	21
6 LAYOUT/CONTENT OF THE WORK PLAN	22
PART 2: ADMINISTRATIVE DETAILS	22
1 ELIGIBILITY REQUIREMENTS	22
2 ADMINISTRATIVE REQUIREMENTS	23
2.1 <i>Different ways to submit a tender</i>	23
2.2 <i>Joint tenders and subcontracting</i>	24
2.3 <i>Identification of the tenderer</i>	24
3 SIGNATURE OF THE TENDER	26
4 LAYOUT OF THE TENDER	26
5 EVALUATION OF TENDERS	27
5.1 <i>Exclusion criteria</i>	28
5.2 <i>Selection criteria</i>	32
5.3 <i>Award criteria</i>	34
6 AWARD OF THE CONTRACT	37
7 PAYMENT AND STANDARD CONTRACT	37
8 VALIDITY OF THE TENDER	38
9 ADDITIONAL PROVISIONS	38
10 LIQUIDATED DAMAGES: SEE ARTICLE II.12 OF THE MODEL CONTRACT	38
11 NO OBLIGATION TO AWARD THE CONTRACT	38
12 RESULTS	39
ANNEX 1: ADMINISTRATIVE IDENTIFICATION FORM	40
ANNEX 2: LEGAL ENTITIES FORM	41
ANNEX 3: BANK IDENTIFICATION FORM	41
ANNEX 4: DECLARATION OF HONOUR	42
ANNEX 5: POWER OF ATTORNEY	45
ANNEX 6A: LETTER OF INTENT FOR SUB-CONTRACTORS	47
ANNEX 6B: LETTER OF INTENT FOR EXTERNAL EXPERTS	48
ANNEX 7: CHECK LIST OF DOCUMENTS TO BE SUBMITTED	49
ANNEX 8: E-PRIOR DESCRIPTION	51
ANNEX 9: COVER LETTER FOR THE TENDER	53
ANNEX 10: TEMPLATE STUDY FINAL REPORT OR EXECUTIVE SUMMARY	55

PART 1: TECHNICAL DESCRIPTION

1 CONTEXT

1.1. General Context

In times of social and political unrest, governments of mature and nascent democracies are increasingly tempted to reduce freedom of speech and unrestricted access to information, both offline and online.

It is undoubted that Internet and more broadly Information and Communication Technologies (ICT's) can be conducive to a more effective protection and exercise of human rights across borders, facilitating freedom of expression and serving as a catalyst for social change, cultural diversity, political expression and democratic prosperity.

However, the opportunities for pluralism and diversity brought about by these technological developments are not risk-free. At the same time that the Internet has opened up a platform for journalists, bloggers, human rights defenders, political activists and citizens to make their voices heard, it has also allowed the use of sophisticated censorship and surveillance methods by non-democratic regimes to silent political criticism.

It is in that scenario that ICTs are an essential contributing factor for the creation of positive dynamics among citizens, freedom and democracy, as well as an unprecedented enabler of dialogue: a key element in society that requires ensuring that all parties can communicate, access and exchange information without restrictions, gateways or filters, and with appropriate privacy and security protections.

DG CONNECT, in close cooperation with other services (DG Development and Cooperation; DG Enterprise) and the European External Action Service (EEAS), has put in place the No-Disconnect Strategy. The goal of this policy toolkit is to provide on-going support to counter-censorship initiatives to facilitate the role of **activists, political dissidents, bloggers, journalists and citizens living and/or operating in high-risk environments**, making operational its commitment to uphold human rights and fundamental freedoms online. This way, the No-Disconnect Strategy embraces the wider EU strategy for Human Rights.¹

The No-Disconnect Strategy is part of the integrated response of the European Union to the events that unfolded in the Middle East and North African region during the Arab Spring to support and advance human rights and democracy in the region, as envisaged in the Joint Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy "**A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean**" (COM(2011) 200)².

1

¹ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0200:FIN:EN:PDF>

Currently, the geographical scope of the Strategy is not limited to the aforementioned region, but operates at global scale given the fact that the implementation of the No-Disconnect Strategy is achieved **in cooperation with other Services and through EU global instruments** such as the **European Instrument for Democracy and Human Rights**³ led by DG Development and Cooperation; and the **EU Strategic Framework on Human Rights and Democracy**, led by the European External Action Service.⁴

1.2. Specific Context

Keeping track of worldwide developments in the area of cyber censorship and establishing the link between Internet restrictions and violations of human rights can be greatly enhanced by a global monitoring system to develop «cartography» of digital repression, capable of mapping events in the cyber-geography of Internet through intelligence gathering.

A truly European capability for situational awareness that **provides near-real time monitoring and visualization tools to increase the understanding of the state of Internet censorship can help EU decision-makers to obtain high-quality information and fine-tune early-warning capabilities necessary to better perform their functions**, particularly in those cases which may require EU integrated and multi-level intervention. Information that is quick, actionable and contextualized can ensure that institutional actions are tailored to reality and that appropriate awareness is created on outstanding technological, political, social, legal, media, policy and human rights related cyber censorship issues.

Through targeted event monitoring, not only EU Institutions but also digital activists, bloggers, journalists, human rights defenders, the open source community, researchers as well as many other stakeholders involved in the area of digital freedoms and Internet openness, will **gain full situational awareness of the threat landscape and type of environment in which they operate, in order to make sound decisions and put in place fast response schemes in the event of a wide array of restrictions** : a sharp increase of human rights violations in a given region such as crackdowns on civil society ; the enforcement of Internet restrictive policies and regulations ; court cases and wrongful detentions/imprisonments ; cyber-attacks to servers hosting politically sensitive content ; or Internet connectivity shutdowns, among others.

One of the reasons behind this technological effort is that Internet and other ICT's have become key instruments for tracking political events and media; for crisis management and mapping; for disaster response ; for monitoring; for the development of preventive capabilities and risk assessments ; or for the support of democratization processes.

These capabilities can also be applied to **events affecting negatively the integrity of Internet infrastructure**, like Domain name system (DNS) filtering, state sponsored attacks to cyber activists systems or filtering blanket laws, for instance, to address questions of overall **Internet security, resilience and stability**. Internet can potentially be used for purposes that are inconsistent with fundamental values as well as inconsistent with basic Internet resilience and stability principles, adversely affecting the performance of

³ http://ec.europa.eu/europeaid/how/finance/eidhr_en.htm

⁴ http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

critical systems and diminishing Internet security and stability as a whole: **it can be argued that blocking and filtering can impair the architectural principles of the Internet and cause harmful (collateral) effects to other systems.** The Cooperative Association for Internet Data Analysis (CAIDA) has also accomplished research in the field of country-wide Internet outages caused by censorship⁵. Others have focused on studying the collateral damages of censorship by DNS injection.⁶

Last but not least, monitoring Internet censorship and its environment, both at the level of network infrastructure / network traffic and “on the ground”, can **reinforce EU’s evidence-based approach to policy making as well as support the implementation of a human rights based approach**, whereby human rights considerations and indicators can be factored in the European Union’s Internet and ICT policy development activities, among others.

It is therefore a priority for the European Union to: a) ensure the availability of Internet and other ICT’s as well as their use without arbitrary interference; and b) gather the necessary data to construct a global view of the cyber geography of censorship and its dynamics through targeted monitoring.

1.3.Examples of organisations and existing projects in the area of Internet monitoring

The European Commission has funded several Framework Programme research projects in the area of Internet and event monitoring. In particular, the 7th Research Framework Programme (FP7) has provided support to projects like EVERGROW (www.evergrow.org) and LOBSTER (www.ist-lobster.org); ETOMIC (www.etomic.org) -subproject of EVERGROW-; DIMES (www.netdimes.org); MOME (www.ist-mome.org); MOMENT ("www.fp7-moment.eu/"); perfSONAR (<http://www.perfsonar.net/> for network performance monitoring in federated environments, developing services acting as an intermediate layer between the performance measurement tools and the diagnostic or visualization applications; or TRAMMS -Traffic Measurements and Models in Multi-Service Networks- (<http://projects.celtic-initiative.org/tramms/>).

The European Parliament asks regularly the European Commission to implement pilot projects related to media freedom and pluralism. For instance, the European Commission was asked in 2013 to implement two pilot projects, on the Media Pluralism Monitoring Tool (09 02 07) and on a European Centre for Press and Media Freedom (33 02 10). It is possible that pilot projects in this area could also be foreseen by the budget of the European Union in the following years.

The U.S. Cooperative Association for Internet Data Analysis (CAIDA) addresses topics related to Internet infrastructure level measurements and analysis to understand traffic trends affecting those infrastructures. Ark (Archipelago Measurement Infrastructure) is CAIDA's active measurement infrastructure to reduce the effort needed to develop and deploy sophisticated large-scale measurements on a security-hardened distributed platform (<http://www.caida.org/home/>).

⁵ http://www.caida.org/publications/presentations/2011/analysis_internet_outages_censorship/

⁶ <http://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf>

Most of the above mentioned initiatives and projects focus on monitoring Internet mainly at the lower OSI model layers⁷. Lately the importance of collecting Internet data and information on traffic at higher layers and « on the ground » to obtain statistical data on Internet usage and usage of Internet applications, has grown considerably and currently attracts the attention of Internet researchers, advocates, industry, as well as of policy makers.

The European Commission has already launched in this context a study on « **Statistical methodologies on Internet as a source of data gathering** » - SMART 2010/0030, with the aim to test the feasibility of new forms of internet-based data collection that could enrich the efforts to monitor the take-up of ICT by social actors as well as the main impacts of ICT based applications and services⁸; and a study on « **European Internet traffic: monitoring tools and analysis** » - SMART 2012/0046, for the mapping of existing Internet monitoring tools and methodologies and to determine the sort of federated monitoring models that can be applied in Europe given the large amount of projects already active in the field.⁹

Examples of organizations and existing projects with monitoring capabilities not funded by the Commission and directly related with the main objectives of this call for tenders are : Govcom: <http://www.govcom.org/>; Free Press Unlimited: <https://www.freepressunlimited.org/en/>; Herdict : <http://www.herdict.org/>; Digital Humanitarian Network : <http://digitalhumanitarians.com/>; Ranking Digital Rights : <http://rankingdigitalrights.org/>; RIPE NCC Atlas : <https://atlas.ripe.net/>; Oxford Internet Institute : [http://www.oii.ox.ac.uk/people/?id=165](http://www.oii.ox.ac.uk/people/?id=165;); Ushahidi : [http://www.ushahidi.com/products](http://www.ushahidi.com/products;); Internews : <http://www.internews.eu/>; FIDH Worldwide Human Rights Movement : <http://www.fidh.org/-english->; IFEX : <http://www.ifex.org/>; Reporters Without Borders : <http://en.rsf.org/>; Renesys : <http://www.renesys.com/blog/>; Internet and Jurisdiction : <http://www.internetjurisdiction.net/observatory/>; ChokePoint Project : <https://chokepointproject.net/>; Arbor Networks Atlas : <http://atlas.arbor.net/>; Team Cymru : <https://www.team-cymru.org/Monitoring/>; Threatened Voices : <http://threatened.globalvoicesonline.org/>; Privacy International : <https://www.privacyinternational.org/projects/global-surveillance-monitor>; Recorded Future : <https://www.recordedfuture.com/>; Analysis Intelligence : <http://analysisintelligence.com/>; ICT4Peace Foundation : <http://ict4peace.org/whatwedo>; Nexa Center Neubot : <http://nexa.polito.it/neubot>; European University Institute : <http://www.hf.uio.no/imk/english/research/center/media-innovations/news/workshop-icts-and-the-global-governance-of-peace-and-security.html>; GreatFire : <https://en.greatfire.org/>; Citizen Lab : <https://citizenlab.org/>; OpenNet Initiative : <https://opennet.net/about-filtering>; Frontline Defenders : <http://www.frontlinedefenders.org/>; Index on Censorship : <http://www.indexoncensorship.org/>; Article 19 : <http://www.article19.org/>; Open Observatory of Network Interference : <https://ooni.torproject.org/>; Institute for Democracy and Conflict Resolution : <http://www.idcr.org.uk/resources-links/data>; The Web Index : <http://thewebindex.org/>; Telecoms Sans Frontiers : <http://www.tsfi.org/en>; Tactical Technology Collective : <https://www.tacticaltech.org/>; iilab : <https://iilab.org/>; The Guardian Project : <https://guardianproject.info/>; Open Internet Tools : <http://openitp.org/>;

⁷ http://en.wikipedia.org/wiki/OSI_model

⁸ http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=6027&language=default

⁹ http://cordis.europa.eu/fp7/ict/fire/calls/studies/2012/0046-internet-traffic/led-smart-2012-0046_en.html

Small Media : <http://smallmediafoundation.com/projects>; Committee to Protect Journalists : <http://www.cpj.org/>; International Commission of Jurists : <http://www.icj.org/>; World Press Freedom Committee : <http://www.wpfc.org/index.php?q=node/10>.

2 OBJECTIVES

The tender "European capability for situational awareness" (ECSA) is aimed at providing to the European commission the necessary information to evaluate the feasibility of creating a **European federation for cyber-censorship and human rights monitoring and the systems infrastructure necessary to that end**. As such, the tasks of the study will address the definition of the governance framework and systems infrastructure that should govern and support the operations of a possible federation. In order to translate reality into a cartography of cyber-censorship, the federation would be anchored in a dynamic platform -controlled from a dashboard-, where a federated network of partners with Internet and censorship monitoring capabilities will aggregate a variety of clearly defined sets of data (including open data and big data) related to the location and intensity of cyber-censorship and surveillance in non-democratic countries or countries where human rights are most at risk. The data gathering will have two tracks, the first one addressing restrictions/disruptions on internet and ICT infrastructure, access, traffic and content, overlaid with a second track of contextual data of political, social, legal, regulatory, policy, media or human rights nature, related to the internet or not. The reliable and near-real time information mashed-up in the dashboard will be presented in a user-friendly manner and in different layers: interactive visualizations through live maps; alarms; subject-matter snapshot reports and geographical snapshot reports. This type of capability is expected to enhance the early-warning, decision-making and policy making skills of EU policy makers and strengthen the level of situational awareness of stakeholders such as digital activists or human rights defenders.

When drafting the offer, it is recommended that TENDERERS take into account the following long-term objectives or expected contributions of the tender "European Capability for Situational Awareness" to EU specific objectives:

- Enhancement of evidence-based policy making based on reliable information
- Support to the implementation of Human Rights-based approaches
- Reinforcement of early-warning capabilities and emergency response
- Optimization of resources and tailored targeted grant support in areas where human rights are most at risk in terms of cyber censorship
- Reinforcement of capabilities to ensure global Internet connectivity
- Ensure Internet security, resilience and stability
- Provide methods for network measurement
- Increase of situational awareness of actors affected by the complexity of cyber censorship, in particular of policy-makers, digital activists and human rights defenders
- Provide capabilities for crisis mapping

A brief analysis of the current Internet monitoring ecosystem (including news/media, human rights, filtering and surveillance, traffic, security, legal or regulatory monitoring among others) suggests a rather scattered and haphazard scenario with several players (research centres, NGO's, private sector or specific constituencies) but with little or no federation vision. The results of individual projects could be stepped-up for the protection of fundamental freedoms online by means of a simple federation effort. The joint work of

the various existing initiatives can play a decisive role in observing the complexity of cyber-censorship from an interdisciplinary and holistic point of view.

For that reason this study is expected to provide a detailed analysis of the different key constitutive elements of a targeted cyber-Censorship monitoring tool, provide recommendations on implementation and budget and present a small scale prototype or proof-of-concept use case with real data.

The tenderer will have to specify in the proposal:

- TASK 1: A list of Internet censorship monitoring organizations capable to constitute a Federation and a proposal for the structure of such Federation
- TASK 2: A catalogue of data sources and categories
- TASK 3: A proposal of a data governance framework, establishing the protocols that will govern the management of the data collected
- TASK 4: A list of necessary infrastructure, features and functionalities
- TASK 5: A set of recommendations on the implementation of the aforementioned 4 tasks.

More specifically, the tasks to be performed under the contract are as follows:

Task 1 Internet censorship monitoring Federation

To develop a capability for situational awareness it is necessary that the monitoring activity is carried out by the collaborative work of a federated network¹⁰ of organizations with the relevant expertise and active in the field of Internet censorship monitoring (please see examples in Section 1.3). This federated network of organizations will act as data sources of a centralized system for further aggregation and processing. The study should produce a complete and diverse **list of existing projects and organizations** which could be federated for the monitoring, collection and analysis of data related to **Task 2**.

The list must be **accompanied by an analysis of the different data sources and types of data collected by each organization or project, the methods employed, the tools or technological developments already in place, the type of expertise and the target groups.**

This section of the study must also present a **proposal for the structure of the Federation**. At least, it shall contain a roadmap with the steps to create such federation; explain how the federation innovates, builds upon and complements other initiatives; provide a planning on how structural relationships will be ensured; present a membership scalability plan and a sustainability plan; indicate the allocation of rights, responsibilities and resources among members of the Federation; define the incentives for members of the federation; identify a common methodology for data gathering and processing based on open standards, protocols and API's, and propose 5 individual members to constitute an "Advisory Group" that will guide the activities of the future federation during the execution of the contract.

¹⁰ "Federation" or "Federated network" are to be understood as a broad group of different organizations, with different capabilities, some of which might be partners or former co-operators, but which decide to partner specifically with ECSA.

For the purpose of this task (and to support the achievement of **Tasks 2-4**), the contractor will have to **run a consultation** targeting Internet (censorship, surveillance and security) monitoring on how to best achieve the objectives of this tender immediately after the start of the contract and during the first 4 months after the start of the contract, followed by the organisation of a **workshop to showcase the results and gather additional input from attendees**. The results of the consultation and the workshop will be presented within the content of the **First Interim Study Report**.

This section of the study must also **present** a proposal for proportional allocation of roles, responsibilities and resources among members **of the** federation.

This part of the study should be able to reply to the following questions, taking into account the context outlined in **Section 1**:

- What monitoring organizations, facilities and networks do exist primarily in Europe (28 Member States)?
- What are the main monitoring capabilities of those existing initiatives?
- What sort of federated monitoring models can be applied in Europe and what is the best way to implement them?

Task 2 Data Sources catalogue

Taking into account the results of the consultation, the study should produce a **comprehensive list of data sources and categories to be monitored for the enhancement of human rights and effective exercise of fundamental freedoms online**. Those data sources and categories will be main sources of information for the central monitoring system, and therefore ensuring their richness as well as the variety of the aggregators is a key requirement. While defining the list, Contractors will have to take into account the following conditions:

- The event monitoring activity and the data gathering will happen at **two levels**:

a) The first level relates to the “**state of the Internet infrastructure, connectivity and access**”, in order to have a near-real-time understanding of network disruptions and traffic alterations in the form of blocking; filtering; connectivity blackouts or slowdowns; power outages; cyber-attacks and security events including attacks on activists’ networks via Distributed Denial of Service attacks, spyware or malware; countries passing laws or applying measures with a negative impact on Internet infrastructure and on its resilience, security and stability; cyber censorship and surveillance technological developments; state-led cyber-attacks, etc.

This track must provide **early-warning capabilities, enhance incident response** schemes and ensure **network connectivity** in the event of disruptions, besides providing a new source of information about **Internet security and infrastructure incidents**. It shall gather reliable data concerning the "cyber-geography" of Internet infrastructure, traffic, access and connectivity taking into account that Internet can potentially be used for purposes that are inconsistent with fundamental rights as well as inconsistent with basic Internet resilience and stability principles, thus adversely affecting the integrity of the Internet as a whole.

b) The second level relates to “**what is happening on the ground**”, to have a near-real-time understanding of events and developments taking place in connection with censorship and surveillance but from the perspective of human rights organizations, domestic and international media networks or outlets, legal, policy, research organizations and democracy advocates. Monitoring activities will address locations where there are grave concerns over intense citizen surveillance or illegitimate censorship of the Internet and other electronic communication technologies and will monitor, for instance: laws and policies affecting the use of ICT for the exercise and protection of human rights; media freedom and pluralism constraints; relevant political events affecting digital freedoms; arrest of activists and journalists in connection to ICT blocked sites; different types of restrictions to freedom of expression; court rulings; illegal detentions; unrest in time of elections; crack-downs on protesters and a wide array of other human rights violations.

This track must provide early-warning capabilities, support evidence and human rights based approaches to Internet policy-making; enhance crisis prevention and management activities, support democracy building and advocacy campaigns and ensure that ICTs are at the disposal of human rights. It shall gather reliable data across actors and organizations directly involved in digital freedoms and the defense of human rights on the ground, as well as from research and academic institutions, legal centers or organizations, private security companies and media actors of all sorts.

- As indicated above, data can be gathered from a wide variety of sources to be defined, such as public sources using Open Data, Big Data and Scientific Data; from private entities, civil society, Academia, actors on the ground, etc. Without the intention of limiting the categories of data to the ones referred below, there are a number of data sets that at least should be monitored:

1. **Technical data:** Internet infrastructure measurement; connection speed; Internet routing data; correlation of routing data with other intelligence; jitter; traffic latencies; packet loss; packet interception; wrong query resolving; network connectivity shutdowns and slowdowns; state of “health” of the DNS and BGP systems; impact of implementation of DNS-level filtering and blocking measures; surveillance technology producers and trade operations; IP traffic restrictions; proxy censorship; Internet backbone performance; Denial of Service attacks; politically-motivated attacks; malware activity; attacks to activists or media networks; domain de-registration; server takedowns; URLs intervened; targeted redirections; network outages; or power grid failures; domains seized.
2. **Internet tools data:** restrictions on websites that provide e-mail or other applications like social networks; web hosting; search engines; translation services; VoIP services; circumvention tools; security software; anonymizers; security and privacy training materials; P2P file-sharing, chat or IMS.
3. **Political data:** unlawful restrictions applied to websites expressing views contrary to the government and government opposition groups; human rights related content such as advocacy, abuses, women liberties; freedom of expression; minority rights; religious movements; foreign policy; political transformations and elections; ethnic groups; history; economics; international organizations; NGOs, activists and human rights defenders; political parties and opposition parties; quality of governmental organizations and judicial system; elections data.

4. **Conflict/Security data:** armed conflicts; border disputes; extremist and separatist movements; government militias; military operations; cyber capabilities; cyber-war; data loss; hosting disruptions; malware; spyware.
5. **Legal and Policy data:** legislative developments related to censorship and surveillance; laws to restrict of freedom of expression; court rulings; possibilities to appeal; Internet rights; possibilities to report blocked content like whistle-blowing services; judicial system monitoring; IPR enforcement; Law Enforcement Agencies; arrests; Internet policy, abusive application and/or criminal defamation laws and disproportionate civil sanctions, including laws related to the criticism of politicians, abusive invocation of public morality or national security (including protection of the nation or national values or incorrect application of hate speech laws)
6. **Business data:** Internet and ICT industry practices affecting human rights; Business and Human Rights initiatives and guidelines; private censorship; or dual-use export controls.
7. **Social/Human Rights data:** sexual content; minorities and women's rights; gaming; gambling; dating sites; drugs and alcohol; public health; sensitive or controversial history, art and literature; environmental issues; hate speech; LGBTI; sex education and family planning; pornography; activism; freedom of association; hacking or topics perceived as sensitive or offensive.
8. **Media data:** media intelligence; social networks; local and foreign press; media outlets; news and video platforms; freedom of expression and media freedom and pluralism; blogging domains; platforms and services; web hosting sites; satellite blocking or jamming; multimedia sharing platforms or restrictions on allocation of spectrum, harassment, intimidation and fostering of self-censorship, impunity for crimes against media actors, media ownership and/or concentration endangering the possibility of independent media

This part of the study should be able to reply to the following questions, taking into the context outlined in **Section 1** and in **Section 2 - Task 1**:

- What data sources and categories are necessary (including the ones referred to in the text above and beyond those if appropriate), whether they are all accessible and to whom are they available?
- What are the data sources and categories which the Federation proposed in Task 1 can provide and what are the gaps as compared to this analysis?
- How will the gathering of such data be organized?

Task 3 Data Governance Framework (Data Protocol)

The contractor should present a coherent **proposal for the Data Governance framework applicable to the data gathered**. The framework must be based on **objective data governance standards** to ensure the quality of the **data collection, processing, storage, organization, access, display and communication**.

At least, the data governance framework must determine applicable criteria to issues of: data collection; data ownership; data quality and quantity; processing; storage;

digitalization; presentation; data verification; data security; anonymity; different types of access to data (roles); duration of access; restricted uses; fair and ethical uses; “do not harm” principle; responsibility for damages; disclosure obligations; enforcement; transparency vs. security; data retention or data loss. The contractors can **propose the inclusion of additional factors in the data governance framework** to ensure an efficient and safe governance of data resources.

The study should contain an analysis of the possibility to set up, on top of the open database, an **additional layer of information for restricted use of the EU institutions and containing restricted EU information and sensitive or confidential information coming from operations on the ground**. The contractor should make **recommendations as regards this issue in Task 5**.

In addition, the contractors should present a **proposal for implementation of the suggested Data Governance Framework**, clearly indicating the relationship of such data governance activities with the role of members of the Federation and the necessary software and hardware infrastructure (for this purpose it is necessary to align the content of this study task with the technical and infrastructure specifications, features and functionalities requested in **Task 4**).

This part of the study should be able to reply to the following questions, taking into the context outlined in **Section 1** and in **Section 2 -Task 1** and **Task 2**:

- What are the main elements that should be taken into account by an optimal data governance model?
- Are there data governance standards that can be used for this particular case?
- Do all data sets and sources need the same level of protection?
- What kind of security measures need to be put in place?
- How will the data governance model be implemented among members of the Federation and what is the necessary infrastructure to make it operative?

Task 4 Technical and infrastructure specifications, features and functionalities

The contractor should present a list with the technical and infrastructure requirements, features and functionalities necessary to articulate the work of the Federation. Specific requirements may apply to the collection and analysis of data, the implementation of the data governance framework and the management of the monitoring system via the dashboard, supported with online live-Map visualisations, alarms and targeted reporting.

The study should pay special attention to the implementation of the following requirements:

- The definition of the management system architecture.
- The definition of a data collection system, capable of performing data analysis to find similitudes and connections among data and to contextualize information (i.e.: semantic analysis, data mining, sentiment analysis, etc.. in order to identify policy, legal, human rights or media trends, among others).
- The implementation of a dashboard, capable to seamlessly aggregate and contextualise data coming from a variety of sources and stakeholders, acting as a control panel of the monitoring system.

- The implementation of online interactive visualisations by means of Live-Maps. This map, accessible online, must be the graphical representation of the data gathered, reflecting on a real cartography of Internet censorship. The Map should give the possibility to consult a version with all the aggregated data, or versions presented in a multi-layered manner depending on the category of data.
- The definition of the security measures applicable to the monitoring system and the means to ensure online availability of the visualizations.
- The generation of alarms, and easy-to-read material such as subject-matter snapshot reports and geographical snapshot reports, to respond swiftly to situational awareness needs. The presentation of the information must be done in a user-friendly, meaningful, comparable manner, and in formats easy to digest and review, adapted to different levels of expertise.
- The implementation of a repository of “processed information” (reports); academic research in the field and any other ready-made material or information concerning cyber-Censorship by themes or geographical locations.
- The use of open standards, (preference for W3C and/or IETF standards) and protocols to ensure quick and easy federation of projects; smooth integration with other projects, technological developments, monitoring studies accomplished by the **European Commission** (such as the studies referred to in Section 1.3 or the recently launched Global Internet Policy Observatory¹¹ – “**GIPO**”) , as well as by third parties, to extend the features and functions of the monitoring system; and to guarantee full interoperability.
- The use of standardises Applications Programming Interfaces (API’s) so that third parties can autonomously use the information provided by the monitoring system to build or federate their own services.
- The specific software and hardware requirements, including hosting (redundant) requirements.
- The possibility to integrate mobile applications that facilitate the relay of information from the ground to the monitoring system.
- **The presentation of a DEMO of the monitoring environment studied supported with a visual map and using real data, as proof-of-concept use case.**

With regard to **features** and functionalities, the contractor is free to determine the way in which the monitoring system will be designed (taking into account the basic requirements outlined above) in order to achieve, at least, the following goals:

- a) Monitor and map censorship and surveillance in several geographic locations.
- b) Map high-risk countries or destinations where dual-use products are traded for its use in connection with human rights violations.
- c) Monitor, map and collect notifications of human rights violations with the support of ICT tools and provide secure channels for Human Rights defenders to share and communicate information.
- d) Monitor, map and measure network incidents and network attacks (including those affecting systems of human rights organizations and activists).
- e) Monitor threats to Internet security, resilience and stability and where possible, establish their connection with human rights violations.

¹¹ <https://ec.europa.eu/digital-agenda/en/news/commission-plans-guide-through-global-internet-policy-labyrinth>

- f) Develop an early warning systems based human rights violations through ICT as key indicators.
- g) Monitoring restrictions of the Internet, media and ICT in times of elections.
- h) Monitor developments in internet policy and Internet regulation in target countries and their implementation: i.e.: new laws passed or amended affecting online rights.
- i) Publication of timely reports and alarms on relevant Internet policy, Internet security and human rights related events.
- j) Publication of timely reports and yearly reports analyzing the information gathered to provide an expert analysis on the state of global Internet censorship and of the gravest restrictions and human rights violations related to the use of Internet and other ICT's.
- k) Enable early detection of incidents, diagnosis of connectivity problems as well as security breaches, allowing for quick and adequate mitigation and response strategies.
- l) Improve the way in which ICTs facilitate effective communication in case of crisis management to link professionals, communities and actors involved in humanitarian and peace-building operations.
- m) Support the work of circumvention tools and privacy enhancing technologies in adapting to new or evolving threat landscapes.
- n) Provide situational awareness to digital activists and human rights defenders.
- o) Help organizations working in the field of cyber censorship further refine their research on the ground and further tailor their campaigning activities and the deployment of tools.

Task 5 Recommendations

The contractors should provide a list of recommendations based on the assessment of the previous tasks. The recommendations will have as a prime target the best way to proceed with the **implementation of all the study tasks (1-4) once assessed, with a view to enable the creation of a European Federation for Cyber-censorship and Human Rights monitoring** and will have to address the following issues:

- Creation of a European federation of Internet monitoring organizations and projects and identification of main stakeholders among the ones listed in response to **Task 1**.
- Creation of a complete data sources and categories catalogue for the purpose of Internet censorship monitoring based on the response to **Task 2**.
- Establishment of the appropriate data governance framework based on the response to **Task 3**.
- Implementation of the federation, data catalogue and data governance model through the necessary technical infrastructure, based on the response to **Task 4**.
- Basic necessary features/functionalities and scalability options based on the response to **Task 4**.
- Estimated budget and implementation timeline (roadmap)

With regard to the **Methodology**, the study should be developed following a clear methodology covering all aspects/tasks of the study. Tenderers are free to propose the specific methodology, taking into account the context and objectives of the study and the following conditions:

- The balance between the efforts devoted to each specific objective of the study should be reasonable and well justified.

- The analysis of today's situation should build on existing projects, state of the art, analysis and sources of information.
- More generally, the study should be based on data from a variety of sources such as company, industry, government, academia, research, open source community, journals, human rights organizations, market studies, etc. It should include information from literature reviews, discussions, interviews, workshops, research, projects or any other relevant source related to key stakeholders in the field of Internet infrastructure and Internet censorship monitoring. Efficient use of available networks should be made by liaising with relevant stakeholder groups such as the examples referred to in Section 1.3

In addition to the requirements specified above, TENDERERS should in their offers:

- Demonstrate their understanding of the objectives
- Justify their expertise in the field of Internet censorship and in monitoring
- Propose a roadmap/workplan that is reliable but also sustainable

3 DURATION

Duration of the tasks must not exceed 23 months and is subject to the provisions of Article I.2.3 of the contract.

For study contracts, please note that the approval period of the final study/progress report (whichever is the latest) should be added to the duration.

4 DELIVERABLES, MEETINGS AND TIMETABLE

4.1 Deliverables

4.1.1 The deliverables listed below must be provided by the contractor:

Inception Report, specifying the methodology, resources and objectives provided in the tender in accordance with the indications provided by the Commission during the inception meeting (see section 4.2 below). A draft of the report shall be made available to the Commission's services for information 5 working days before the inception meeting. The final report should take into account all observations made by the Commission. The Inception Report shall be made available within 2weeks after the inception meeting.

First Interim Study Report which will cover the findings for **Task1** (including an Annex with the results of the consultation and the workshop) and the interim findings for all other tasks carried out during the first 6 months. It will also include the workshop report which shall contain the presentations, position papers and preparatory papers; a high quality synthesis of the discussions; and the list of participants of the workshop mentioned under section 4.2. A draft of the report shall be made available to the Commission's services 5 working days before the first interim meeting in month 7 (described in section 4.2 below). The report should be finalised after the meeting taking into account all observations and comments raised at the meeting. The final first Interim Study Report shall be submitted to the Commission's services within 2 weeks after the first interim meeting.

Second Interim Study Report which will cover the findings for **Task 2** and **Task 3** and the interim findings for all other tasks carried out between month 6 and month 12. A draft of the report shall be made available to the Commission's services 5 working days before the second interim meeting in month 13 (described in section 4.2 below). The report should be finalised after the meeting taking into account all observations and comments raised at the meeting. The final second Interim Study Report shall be submitted to the Commission's services within 2 weeks after the second interim meeting.

Interim Progress Report, describing the execution of the study according to the management plan until month 12. The description should include comprehensive monitoring tables showing planned vs. executed resources, highlight any deviations and justify them and make a clear link between the objectives of the study, and the consumed resources. The report needs to be supported by any relevant material e.g. time-sheets on person/days consumption, travel details, use of consumables, infrastructure, etc. The interim progress report is for Commission's monitoring purposes. The interim progress report shall be made available to the Commission's services within 13 months after signature of the contract by the last contracting party.

Technical Report outlining the infrastructural setup and detailing the technical approach to **Task 4**, including the **proof-of-concept use case**. The report should describe the objectives, the rationale of choice of software and hardware; contain an explanation of the combination of monitoring methods and tools and how they will be finally implemented; and present an evaluation of resources based on price and performance metrics. The report should highlight and explain in detail how the contractor is achieving the requirements set forth in Task 4 and include a preliminary assessment of the different features that the monitoring system should have. The technical report shall be made available to the Commission's services within 15 months after signature of the contract by the last contracting party.

Final Progress Report, with the same format and content as the interim progress report but for the total duration of the study, and containing updated information. The final progress report shall be made available to the Commission's services within 18 months after signature of the contract by the last contracting party.

Final study report

A first draft of the final study report, taking into account the input and feedback received over the previous 18 months, shall be made available to the Commission's Services 5 working days before the final meeting foreseen in month 19. The report should be finalised after the meeting taking into account all observations and comments raised at the meeting. The final study report shall be submitted to the Commission's services within 1 month after the final meeting.

Final data set

The final data should be provided as structured data in a machine readable format¹² (e.g. in the form of a spread sheet and/or an RDF file) for Commission internal usage and **for publishing** on the [Open Data Portal](#), in compliance with Commission Decision (2011/833/EU). If third parties' rights don't allow their publication as open data, the bidder should describe in the offer the subpart that will be provided to the Commission free of rights for publication and the part that will remain for internal use.

The data delivered should be **linked to data resources** external to the scope of the study, preferably data and semantic resources from the Commission's own data portal or from the upcoming pan-European portal. The bidder should describe in the offer the approach they will adopt for data linking¹³.

With regard to data **granularity** the bidder should include a dataset with all the information on the variables listed in Task 2 above. In case of statistical data that could be used to derive/compute indicator (e.g. for benchmarking the Digital Agenda), the contractor should use the following template based on the DataCube vocabulary (add ref to <http://ec.europa.eu/digital-agenda/en/download-data>).

The data delivered should **include the appropriate metadata** (e.g. description of the dataset, definition, label and sources for the variables, notes) to facilitate reuse and publication

Concerning **anonymisation of microdata**, the bidder will have to provide clear identification of the units analysed/interviewed, for example in view of future data collections concerning the same units, or in the sense of requiring an anonymised version of the microdata for publication purposes.

4.1.2 Report format

All deliverables must be written in English.

All reports should be consistent in style (headings, margins, citations, bibliography, etc.) and contain a short executive summary. The contractor is required to properly apply quotation techniques and particular care will be taken to verify improper re-use of existing material.

All reports will be submitted in 2 paper copies and in electronic format (.doc, .xls, .ppt or equivalents in open formats). Exchange of advance copies as well as other non-formal communications shall take place via electronic mail.

The Commission services will decide the possible dissemination of the findings and conclusions and any other information produced under this assignment.

¹² See definitions for "structured data" and "machine readable" format in art 3 of Commission Decision (2011/833/EU)

¹³ See: http://en.wikipedia.org/wiki/Linked_data and the tutorials proposed on the Commission Open Data Portal: <http://open-data.europa.eu/en/linked-data>

4.1.3 Content

4.1.3.1 Final Study Report

The final study report shall include:

- an abstract of no more than 200 words and an executive summary of maximum 6 pages, both in English and French;
- the following standard disclaimer:

"By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Reproduction is authorised provided the source is acknowledged (optional)

This clause can only be inserted if the following conditions are fulfilled:

- No third-party textual or artistic material is included in the publication without the Copyright holder's prior consent to further dissemination and reuse by other third parties or:

- An additional notice specifies that the reproduction of the third-party textual or artistic material included in the study is prohibited

Copyright © XXXX – European Union. All rights reserved. Certain parts are licensed under conditions to the EU."

Replace XXXX with the year of publication

- Specific identifiers which shall be incorporated on the cover page provided by the Contracting Authority.

The Final Study Report (including abstract and executive summary) shall be provided in 3 bound paper copies including annexes and in a .pdf format suitable for publication by the Commission's services on Commission websites.

4.1.3.2 Publishable executive summary

The publishable executive summary shall be provided in both in English and French and shall include:

- *the following standard disclaimer:*

"By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Reproduction is authorised provided the source is acknowledged. (optional)

This clause can only be inserted if the following conditions are fulfilled:

- No third-party textual or artistic material is included in the publication without the Copyright holder's prior consent to further dissemination and reuse by other third parties or:

- An additional notice specifies that the reproduction of the third-party textual or artistic material included in the study is prohibited

Copyright © XXXX – European Union. All rights reserved. Certain parts are licensed under conditions to the EU."

Replace XXXX with the year of publication

- Specific identifiers which shall be incorporated on the cover page provided by the Contracting Authority.

4.1.3.3 Abstract

The abstract provided both in English and French in the Final study report (see point 4.1.3.) in no more than 200 words shall be provided as well in a separate document for the purpose of the description of the study on the website of the EU Bookshop.

No identifiers shall be incorporated on this file.

4.1.4 Structure

The **Final study report** shall include the following sections:

1. Executive summary
2. Justification and presentation of the adopted methodology for the study
3. The results and analysis of the consultation and workshop of Task 1
4. The result of Task 1
5. The result of Task 2
6. The result of Task 3
7. The result of Task 4
8. The proof-of-concept use case (dashboard + visualization)
9. Recommendations as a result of Task 5
10. Conclusions
11. Annexes

4.1.5 Graphic requirements

The new visual identity applies to all commission services and related bodies.

For graphic requirements please refer to the template provided in the annex 10, "Visual identity template for DG CONNECT studies". The cover page shall be filled in by the contractor in accordance with the instructions provided in the template.

In case you foresee other logos than the Commission logo, the additional logo may only be placed on the cover page of the study if they are one of the following categories:

- a logo duly authorised by the Secretary General and the Director-General for Communication of the European Commission;
- the logo of the author of the study (i.e. the contractor);
- in case of co-branded studies, the logo of a partner organisation involved in the production of the study. In this case, the European Commission's Visual Identity Manual does not apply.

4.2 Meetings and workshops

A schedule of meetings will be agreed with the contractor for this assignment. Such meetings will be attended by representatives of the European Commission, the project manager leader and other members of the contractor's team, as required. Other knowledgeable external experts might be invited to participate by the Commission. The meetings will be chaired by a Commission representative and will take place in *Brussels*.

The aim of the meetings will be to guide the work of the contractor. In particular, they will allow setting-up the initial orientations, review progress in critical milestones and review the deliverables of the assignment.

Within three days following each meeting, the contractor will circulate minutes of the meeting to all participants, together with copies of presentations made during the meeting or other related documents. The minutes shall be concise and concentrate on major decisions and shall list the open action points for the next reporting period.

Inception meeting. It is organised by the Commission's services at the Commission's premises in Brussels within 1 month after signature of the contract by the last contracting party. The contractor will have to finalise the inception report on the basis of the outcome of the inception meeting.

Consultation and Workshop. The contractor is expected to organise one consultation among organizations and projects already active in the field of Internet and Internet censorship monitoring (see examples in Section 1.3) and a workshop to showcase the results of the consultation and gather further insights from interested stakeholders. The consultation will start right after the signature of the contract by the last contracting party and will be closed exactly 4 months afterwards. The workshop will take place in month 5 and will last 1 day. The workshop will take place at the Commission's premises in Brussels. In case and alternative location for the workshop is proposed by the contractor, this has to be agreed by the Commission in advance and to remain within the budget foreseen in the tender.

The aim of the consultation and the workshop is to gather input for Task 1 (but also for the achievement of Task 2, 3 and 4). During the workshop renowned and representative experts in the area of Internet monitoring should discuss the topics related to Task 1, 2, 3 and 4. During the workshop the rationale and choice of the use case should be discussed and analysed.

The aim of the workshop is also to inform relevant stakeholders and experts about the findings of the consultation, validate and collect their views on them, as well as more general views, especially on current and future developments in the area of the study and its policy implications. This will require the contractor preparing a short document and/or a presentation, which will summarise the findings of the consultation and will raise issues for discussion at the workshop. The documentation related to the consultation and the workshop will be included in the workshop report (see section 4.1.1) which will be part of the First Interim Study Report.

Costs related to the following activities and items must be borne by the contractor and included in the price:

- Setting the workshop agenda in cooperation with the Commission;
- Identifying participants and speakers in cooperation with the Commission;
- Inviting speakers and participants;
- Managing the travel and accommodation arrangements for [*up to 2 speakers [and 1 participants]*];
- Financing the travel and accommodation expenses for [*up to 2 speakers [and 1 participants]*];
- Any speakers' fees;
- Cost of providing catering during the workshop;
- Printing and distributing relevant information material for speakers and participants.

First Interim meeting during which the contractor will present the findings for Task 1 (including the results of the consultation and the workshop) and the interim findings for all other tasks carried out during the first 6 months. It will be held within 7 months after signature of the contract by the last contracting party. It will be organised by the Commission's services at the Commission's premises in Brussels. The contractor will have to finalise the first interim study report on the basis of the outcome of the first interim meeting.

Second interim meeting during which the contractor will present the findings for Task 2 and Task 3, and the interim findings for all other tasks carried out between month 6 and month 12. It will be held within 13 months after signature of the contract by the last contracting party. It will be organised by the Commission's services at the Commission's premises in Brussels. The contractor will have to finalise the second interim study report on the basis of the outcome of the second interim meeting.

Technical meeting, during which the contractor will present the findings for Task 4 and showcase progress in the development of the proof-of-concept use case. It will be held within 15 months after signature of the contract by the last contracting party. It will be organised by the Commission's services at the Commission's premises in Brussels. The contractor will have to finalise the final progress report on the basis of the outcome of the technical meeting.

Final meeting during which the contractor will present the final findings and proposed conclusions will be held within 19 months after signature of the contract by the last contracting party. It will be organised by the Commission's services at the Commission's premises in Brussels. The contractor will have to finalise the final study report on the basis of the outcome of the final meeting, **one month afterwards and in any case before the end of month 21.**

Regular conference calls (at least 4). In addition to the meetings to be organised in Brussels, conference calls on the state of progress of the study will take place, when possible and necessary, between representatives from the contractor and the Commission.

Each TENDERER should include costs of attendance of its own representative(s) at all the above meetings and workshop in the financial section of the offer.

4.3 Timetable

Title	Type	Due month
Inception meeting	Meeting	1
Inception report	Report	1
Launch of the consultation	Consultation	1
First conference call	Meeting	4
Workshop	Workshop	5
First interim meeting	Meeting	7
First interim study report – Task 1	Deliverable	7
Second conference call	Meeting	10
Second interim meeting	Meeting	13
Second interim study report – Task 2 and Task 3	Deliverable	13
Interim progress report	Deliverable	13
Third conference call	Meeting	14
Technical meeting	Meeting	15
Technical report	Deliverable	15
Final progress report	Deliverable	18
Fourth conference call	Meeting	18
Final meeting	Meeting	19
Final data set	Deliverable	19
Final study report	Deliverable	20

5 TERMS OF APPROVAL OF REPORTS/DELIVERABLES

5.1 Study report(s)

After reception of each study report included in section 4.1 above, except for the reports linked to payments, the Commission will have 45 calendar days in which:

- to approve it,
- to reject it and request a new report.

If the Commission does not react within this period, the report shall be deemed to be approved.

Where the Commission requests a new report because the one previously submitted has been rejected, this must be submitted within 30 calendar days. The new report shall likewise be subject to the above provisions.

5.2 Progress report(s)

The Commission shall have forty-five days from receipt to approve or reject the progress report(s), and the Contractor shall have 15 days in which to submit additional information or a new report.

5.3 Other Deliverables (consultation, Workshop and technical report)

The Commission shall have 30 days from receipt to approve or reject the deliverable(s), and the Contractor shall have 15 days in which to submit additional information or a new deliverable.

For the reports linked to the payments, we refer to article I.4 of the service contract.

6 LAYOUT/CONTENT OF THE WORK PLAN

TENDERERS should describe in their offers their understanding of the objectives and tasks and present a procedure to achieve Task 1, Task 2, Task 3 and Task 4, supported by a work plan and an implementation roadmap with clear milestones, in accordance with the timing established by the list of deliverables set forth in Section 4.

The work plan should specify the management structure, clear milestones as well as the allocation of responsibilities and resources to each member of the team, including the main contractor and/or sub-contractors or members of the federation. It should include the names of the persons in charge of the different countries where data have to be gathered.

The work plan should include a list of tasks to be performed, with clear and realistic phases and milestones. Resources should be clearly associated to each task.

PART 2: ADMINISTRATIVE DETAILS

1 ELIGIBILITY REQUIREMENTS

The present tender documents are drawn up in respect of the Financial Regulation (EU, Euratom) No 966/2012 of the European Parliament and the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union and repealing Council Regulation (EC, Euratom) No 1605/2002, as well the Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 on the rules of application of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council on the financial rules applicable to the general budget of the Union, hereinafter referred to as the Financial Regulation.

Participation in tendering procedures is open on equal terms to all natural and legal persons from one of the EU Member States and to all natural and legal persons in a third country which has a special agreement with the Union in the field of public procurement on the conditions laid down in that agreement.

Where the Plurilateral Agreement on Government Procurement concluded within the WTO applies, the contracts are also open to nationals of the countries that have ratified this Agreement, on the conditions it lays down.

Operators in third countries which have signed a bilateral or multilateral agreement with the Union in the field of public procurement must be allowed to take part in the tendering procedure on the conditions laid down in that agreement. The Commission will refuse tenders submitted by operators in third countries which have not signed such agreements for the present call for tender.

ADMISSIBILITY OF TENDERS

All the **requirements** related to the **submission and opening of the tenders** are detailed in the invitation to tender (see sections 2, 4 and 8 of the invitation to tender) including:

- *Address and deadline for submission of the tender*
- *Presentation of the offer and Packaging*
- *Opening of the Tenders*

2 ADMINISTRATIVE REQUIREMENTS

A service provider may consider submitting a tender as a single entity or decide to collaborate with other service providers to present a bid: either by submitting a **joint tender** or through **subcontracting**. Tenders may also combine both approaches. Whichever type of bid is chosen, the tender must stipulate the legal status and role of each legal entity in the tender proposed.

2.1 Different ways to submit a tender

Options 1 to 4 below describe the different ways to submit a tender.

Please make sure all required documents and evidences are submitted with your tender.
(Please refer to the checklist in Annex 7)

- Option 1:** Submission by **one tenderer: Private / Public entity / Individual.**
- Option 2:** Submission by **partners** as defined under section 2.2 below.
One must be designated as **lead partner/contractor.**
- Option 3:** Submission by **one tenderer with subcontractors** as defined under section 2.2 below
- Option 4:** Submission by **partners** (one must be designated as lead partner/contractor) **with subcontractors** as defined under section 2.2 below

The tender must include a cover letter (Annex 9) presenting the name of the tenderer (including all entities in case of joint offer as well as their roles) and identified subcontractors if applicable.

2.2 Joint Tenders and Subcontracting

2.2.1 Joint tenders

In case of a joint tender submitted by a group of tenderers, these latter will be regarded as **partners**. If awarded the contract, they will have an equal standing towards the contracting authority in the execution of the contract.

The partnership may take the form of:

- p) a **new legal entity** which will sign the contract with the Commission in case of award
- or
- q) a group of partners not constituting a new legal entity, who via a **power of attorney (Annex 5)**, signed by an authorised representative of each partner (except the lead partner), designate one of the partners as lead partner, and mandate him as lead contractor to sign the contract with the Commission in case of award.

In both cases, all partners shall be considered as tenderers and shall **assume joint and several liability towards the European Commission for the performance of the contract.**

2.2.2 Subcontracting

Subcontracting is a situation where a contract is to be established between the Commission and a service provider and where this service provider, in order to carry out the contract, enters into legal commitments with other legal entities for performing part of the tasks foreseen in the contract.

The tenderer submitting the tender, if awarded the contract, shall become the sole contractor and shall assume **full liability toward the European Commission for the performance of the contract as a whole.** The other service providers will be regarded as subcontractors.

Subcontracting is subject to the provisions of Article II.7 of the model contract annexed to the invitation.

2.3 Identification of the tenderer – List of Forms & Evidences Required

Options 1/2/3/4: Documents to be provided by the single tenderer or lead partner:

- Annex 1: Administrative identification form (ORIGINAL filled in and signed by (an) authorised representative(s))
- Annex 2: Legal Entities form¹⁴ (ORIGINAL filled in, signed by (an) authorised representative(s), and supported by relevant evidences according to the entity concerned, i.e. private/public/individual)
Economic operators already registered as a legal entity in the Commission's files (i.e. they are or have been contractors of the Commission) are not obliged to provide a new form, on the condition that they confirm that no change in the information already provided has occurred. In case of doubt, we recommend submitting a new form.
- Annex 3: Financial Identification form¹⁵ (ORIGINAL filled in according to the instructions contained in this form)
If the corresponding bank account of economic operators is already registered in the Commission's files they are not obliged to provide a new form, on the condition that they confirm that no change in the information already provided has occurred. In case of doubt, we recommend submitting a new form.
- Annex 4: Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest (ORIGINAL filled in and signed by (an) authorised representative(s))
- Legible photocopy of the statutes of the legal entity (for public/private entities)
- Legible photocopy of the notice of **appointment of the persons authorised to represent the tenderer** in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation which applies to the legal entity concerned requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.

Options 2 and 4: documents to be provided by each partner, except the lead partner

- Annex 1: Administrative identification form (ORIGINAL filled in and signed by (an) authorised representative(s))
- Annex 2: Legal Entities form¹⁶ (ORIGINAL filled in, signed by (an) authorised representative(s), and supported by relevant evidences according to the entity concerned, i.e. private/public/individual)

¹⁴

A standard template in each EU language is available at http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

¹⁵

A standard template in each EU language is available http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

Economic operators already registered as a legal entity in the Commission's files (i.e. they are or have been contractors of the Commission) are not obliged to provide a new form, on the condition that they confirm that no change in the information already provided has occurred. In case of doubt, we recommend submitting a new form.

- Annex 4: Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest (ORIGINAL filled in and signed by (an) authorised representative(s))
- Annex 5: Power of attorney (ORIGINAL filled in and signed by (an) authorised representative(s) of each partner)
- Legible photocopy of the statutes of the legal entity (for public/private entities)
- Legible photocopy of the notice of **appointment of the persons authorised to represent the tenderer** in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation which applies to the legal entity concerned requires such publication. Any delegation of this authorisation to another representative not indicated in the official appointment must be evidenced.

Options 3 and 4: Documents to be provided by each subcontractor

- Annex 1: Administrative identification form (ORIGINAL filled in and signed by (an) authorised representative(s))
- Annex 4: Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest (ORIGINAL filled in and signed by (an) authorised representative(s))
- Annex 6a: Letter of intent from each subcontractor (ORIGINAL signed by (an) authorised representative(s)) to confirm their willingness and availability to perform the tasks.

Individual external experts, not part of the tenderer's staff, foreseen to execute a part of the work are also to be considered subcontractors. Individual external experts will have to provide only the letter of intent in Annex 6b (ORIGINAL).

3 SIGNATURE OF THE TENDER

The signature of the single tenderer's or lead partner's authorised representative or representatives (preferably in blue ink) on the administrative identification form (**Annex 1**) will be considered as the signature of the tender, binding the single tenderer or the group of partners to the terms included in the tender.

4 LAYOUT OF THE TENDER

All tenders must be clear, complete and consistent with all the requirements laid down in the tendering documents and **presented in 3 sections** as follows:

4.1 Administrative section

The documentary evidence required in accordance with part 2 section 2, section 3, section 5.1.3 and section 5.2 of the Tender Specifications must be included in the administrative section of the tender. **Tenders not including the necessary evidence may be rejected.** The Commission reserves the right, however, to request clarification or additional evidence in relation to the exclusion and selection stages after the opening within a time limit stipulated in its request and in the conditions explained in section (3) of the invitation to tender.

4.2 Technical section

This section must address all the requirements laid down in Part 1 - Technical description of the tender specifications. Information included here will be used to conduct the qualitative assessment of the tenders on the basis of the technical award criteria listed in section 5.3 below.

The Commission will reject tenders where no technical offers are proposed.

4.3 Financial section

The price quoted must fulfil the following requirements:

A **total** fixed price expressed **in Euro** must be included in the tender.

The price quoted must **be firm and not subject to revision.**

The European Commission, pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Union, is exempt from all duties, taxes and dues, including value added tax (VAT).

Such charges may not therefore be included in the calculation of the price quoted.

VAT 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.

For those countries where national legislation provides an exemption by means of reimbursement, **the amount of VAT is to be shown separately.** 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 Commission is exempt from VAT.

The price quoted shall be subject to the terms set in Article I.3 of the model contract attached.

The price must fall within the scope of these tender specifications and be broken down into unit prices and quantities per each of the following categories:

(a) Professional fees. The daily rates and total number of person-day for each member of staff working on the contract must be specified.

(b) Travel and subsistence expenses (including costs of attendance of future contractor's representative(s) at meetings and/or workshops with the Commission as foreseen in section 4.2, part 1). In the event of travel being necessary to carry out the duties specified in the tender, travel and subsistence expenses shall be paid as indicated in the tender.

(c) Other expenses (outsourced services or supplies e.g. translation expenses, printing expenses, website development, cost of acquiring data etc.)

Tenders involving more than one legal entity, either as partner or subcontractor (including external experts) must specify the categories above for each legal entity.

The Commission will reject tenders where no financial offers are proposed.

The part that the tenderer intends to subcontract shall be precisely indicated and detailed.

The total price quoted cannot exceed EUR 400 000 (four hundred thousand). Tenders with a higher total price will be rejected.

5 EVALUATION OF TENDERS

The evaluation of tenders will be done in accordance with the following subsequent steps:

- The Commission verifies that the **tenderer** is not in one of the situations covered by the exclusion criteria (first step, see section 5.1 below)
- For all tenderers that are not in one of the situations covered by the exclusion criteria, the Commission verifies that the **tenderer** has the appropriate capacities to perform the contract on the basis of the selection criteria (second step, see section 5.2 below)
- For those tenderers that have met the minimum requirements for the selection criteria, the Commission assesses the **tender** on the basis of the award criteria (third step, see section 5.3 below).

5.1 Exclusion Criteria

5.1.1. Pursuant to Article 45(2) of Council Directive 2004/18/EC and to Article 106(1) of the Financial Regulation, the Commission will exclude tenderers from participation in the procurement procedure if:

- (a) they are bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are the subject of proceedings concerning those matters, or are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- (b) they or persons having powers of representation, decision making or control over them have been convicted of an offence concerning their professional conduct by a judgment of a competent authority of a Member State which has the force of *res judicata*;
- (c) they have been guilty of grave professional misconduct proven by any means which the contracting authorities can justify including by decisions of the European Investment Bank and international organisations;

- (d) they are not in compliance with their obligations relating to the payment of social security contributions and the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the contracting authority or those of the country where the contract is to be performed;
- (e) they or persons having powers of representation, decision making or control over them have been the subject of a judgement which has the force of *res judicata* for fraud, corruption, involvement in a criminal organisation, money laundering or any other illegal activity, where such illegal activity is detrimental to the Union's financial interests;
- (f) they are currently subject of an administrative penalty referred to in Article 109(1) of the Financial Regulation.

Points (a) to (d) of the first subparagraph shall not apply in the case of purchase of supplies on particularly advantageous terms from either a supplier which is definitively winding up its business activities, or from the receivers or liquidators of a bankruptcy, through an arrangement with creditors, or through a similar procedure under national law.

Points (b) and (e) of the first subparagraph shall not apply where the candidates or tenderers can demonstrate that adequate measures have been adopted against the persons having powers of representation, decision making or control over them, who are subject to a judgement as referred to in points (b) or (e) of the first subparagraph.

For the purpose of the correct application of paragraph 1, the candidate or tenderer, whenever requested by the contracting authority, shall:

- (a) where the candidate or tenderer is a legal person, provide information on the ownership or on the management, control and power of representation of the legal person and certify that they are not in one of the situations referred to in paragraph 1 of Article 106 of the Financial Regulation;
- (b) where subcontracting is envisaged, certify that the subcontractor is not in one of the situations referred to in paragraph 1 of Article 106 of the Financial Regulation

5.1.2. Pursuant to Article 45(2) of Council Directive 2004/18/EC and Article 107 of the Financial Regulation, a contract shall not be awarded to candidates or tenderers who, during the procurement procedure for this contract:

- (a) are subject to a conflict of interest;
- (b) are guilty of misrepresenting the information required by the contracting authority as a condition of participation in the procurement procedure or fail to supply this information;
- (c) find themselves in one of the situations of exclusion, referred to in Article 106(1) of the Financial Regulation, for this procurement procedure.

5.1.3. Tenderers – including sub-contractors if any - shall provide a declaration on their honour (Annex 4), duly signed and dated, stating that they are not in one of the situations referred to in Article 106(1) or 107 of the Financial Regulation. The tenderers must undertake to inform the Commission, without delay, of any changes with regard to these situations after the date of submission of the tender.

5.1.4. In addition, for contracts of a value higher than EUR 130000, ONLY the tenderer to whom the contract is to be awarded shall confirm the declaration by providing, within a time-limit defined by the contracting authority and preceding the

signature of the contract, the following evidences (if the tender is proposed by partners, these evidences must be submitted by each partner):

9. The contracting authority shall accept as satisfactory evidence that the candidate or tenderer to whom the contract is to be awarded is not in one of the situations described in point (a), (b) or (e) of Article 106(1) of the Financial Regulation, a recent extract from the judicial record or, failing that, a recent equivalent document **issued less than 12 months before the date of the letter informing of the contract award** by a judicial or administrative authority in the country of origin or provenance showing that those requirements are satisfied. Where the tenderer is a legal person and the national legislation of the country in which the tenderer is established does not allow the provision of such documents for legal persons, the documents should be provided for natural persons, such as the company directors or any person with powers of representation, decision making or control in relation to the tenderer. The contracting authority shall accept, as satisfactory evidence that the candidate or tenderer is not in the situation described in point (d) of Article 106(1) of the Financial Regulation, recent certificates or letters issued by the competent authorities of the State concerned, **issued less than 12 months before the date of the letter informing of the contract award**. These documents must provide evidence covering all taxes and social security contributions for which the tenderer is liable, including for example, VAT, income tax (natural persons only), company tax (legal persons only) and social security contributions.
10. Where the document or certificate referred to in the first subparagraph is not issued in the country concerned, it may be replaced by a sworn or, failing that, a solemn statement made by the interested party before a judicial or administrative authority, a notary or a qualified professional body in his country of origin or provenance.

If the tenderer is a legal person, information on the natural persons with power of representation, decision making or control over the legal person shall be provided only upon request by the contracting authority.

Depending on the national legislation of the country in which the candidate or tenderer is established, the documents referred to in paragraphs 1) and 2) shall relate to legal persons and/or natural persons including, where considered necessary by the contracting authority, company directors or any person with powers of representation, decision-making or control in relation to the candidate or tenderer.

In case of doubt on the declaration on the honour provided by the subcontractor(s) in accordance with the indications of point 5.1.3 above, the contracting authority shall request the evidence referred to in points 1) and 2) above from the subcontractor(s).

5.1.5. Administrative and financial penalties

1. **By returning the form in Annex 4 duly signed and dated**, tenderers confirm that they have been notified of the following points: Each institution has a central database containing information on tenderers who have been in one of the situations described under 5.1.1 and 5.1.2 above. The sole purpose of this database is to ensure, in compliance with Union rules on the processing of personal data, that the above-mentioned cases of exclusion are applied correctly. Each institution has access to the databases of the other institutions.

Tenderers and, if they are legal entities, persons who have power of representation, decision-making or control over them, are informed that, should they be in one of the situations mentioned in:

- the Commission Decision of 16.12.2008 on the Early Warning System (EWS) for the use of authorising officers of the Commission and the executive agencies (OJ, L 344, 20.12.2008, p. 125), or
 - the Commission Regulation of 17.12.2008 on the Central Exclusion Database – CED (OJ L 344, 20.12.2008, p.12),
- their personal details (name, given name if natural person, address, legal form and name and given name of the persons with power of representation, decision-making or control, if legal person) may be registered in the EWS only or both in the EWS and CED, and communicated to the persons and entities listed in the above-mentioned Decision and Regulation, in relation to the award or the execution of a procurement contract or a grant agreement or decision.
2. In accordance with Article 109 of the Financial Regulation the contracting authority may impose administrative or financial penalties on the following:
 - (a) contractors, candidates or tenderers in the cases referred to in point (b) of Article 107(1) of the Financial Regulation;
 - (b) contractors who have been declared to be in serious breach of their obligations under contracts covered by the budget.

In all cases, however, the contracting authority shall first give the person concerned an opportunity to present his or her observations.

3. The penalties referred to in paragraph 2 shall be proportionate to the importance of the contract and the seriousness of the misconduct, and may consist in:
 - (a) the exclusion of the candidate or tenderer or contractor concerned from the contracts and grants financed by the budget for a maximum period of ten years; and/or
 - (b) the payment of financial penalties by the candidate or tenderer or contractor up to the value of the contract in question.
4. In accordance with Article 141 of the Regulation laying down the rules of application of the Financial Regulation, the cases referred to in point e) of 5.1.1. above shall include all illegal activities detrimental to the Union's financial interests and be in particular the following:
 - (a) cases of fraud as referred to in Article 1 of the Convention on the protection of the European Communities' financial interests drawn up by Council Act of 26 July 1995 (OJ C 316, 27.11.1995, p. 48);
 - (b) cases of corruption as referred to in Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, drawn up by the Council Act of 26 May 1997 (OJ C 195, 25.6.1997, p. 1);
 - (c) cases of participation in a criminal organisation, as defined in Article 2 of Council Framework Decision 2008/841/JHA (OJ L 300, 11.11.2008, p. 42);
 - (d) cases of money laundering as defined in Article 1 of Council Directive 2005/60/EC of the European Parliament and of the Council (OJ L 309, 25.11.2005, p. 15).;

(e) cases of terrorist offences, offences linked to terrorist activities, and inciting, aiding, abetting or attempting to commit such offences, as defined in Articles 1, 3 and 4 of Council Framework Decision 2002/475/JHA (OJ L 164, 22.6.2002, p.3).

5. Pursuant to article 142 of the Regulation laying down the rules of application of the Financial Regulation, in order to determine duration of exclusion and to ensure compliance with the principle of proportionality, the institution responsible shall take into account in particular the seriousness of the facts, including their impact on the Union's financial interests and image and the time which has elapsed, the duration and recurrence of the offence, the intention or degree of negligence of the entity concerned and the measures taken by the entity concerned to remedy the situation.

When determining the period of exclusion, the institution responsible shall give the candidate or tenderer concerned the opportunity to express their views.

Where the duration of the period of exclusion is determined, in accordance with the applicable law, by the authorities or bodies referred to in Article 108(2) and (3) of the Financial Regulation, the Commission shall apply this duration up to the maximum duration laid down in Article 106(4) of the Financial Regulation.

6. The period referred to in Article 106(4) of the Financial Regulation is set at a maximum of five years, calculated from the following dates:
- (a) from the date of the judgment having the force of res judicata in the cases referred to in points (b) and (e) of Article 106(1) of the Financial Regulation;
 - (b) from the date on which the infringement is committed or, in the case of continuing or repeated infringements, the date on which the infringement cases, in the cases referred to in Article 106(1)(c) of the Financial Regulation where the misconduct relates to contracts with the institution concerned.

For the purposes of point (b) of the sixth subparagraph, if the grave professional misconduct was established by a decision of a public authority or an international organisation, the date of the decision shall prevail.

That period of exclusion may be extended to ten years in the event of a repeated offence within five years of the date referred to in points (a) and (b), subject to paragraph 5.

7. Candidates and tenderers shall be excluded from a procurement and grant procedure as long as they are in one of the situations referred to in points (a) and (d) of Article 106(1) of the Financial Regulation.
8. Pursuant to article 145 of the Regulation laying down the rules of application of the Financial Regulation, without prejudice to the application of penalties laid down in the contract, candidates or tenderers and contractors who have made false declarations, have made substantial errors or committed irregularities or fraud, or have been found in serious breach of their contractual obligations may be excluded from all contracts and grants financed by the Union budget for a maximum of five years from the date on which the infringement is established as confirmed following a contradictory procedure with the candidate, tenderer or contractor.

That period may be extended to ten years in the event of a repeated offence within five years of the date referred to in the first subparagraph.

9. Tenderers or candidates who have made false declarations, have committed substantial errors, irregularities or fraud, may also be subject to financial penalties representing 2% to 10% of the total estimated value of the contract being awarded.

Contractors who have been found in serious breach of their contractual obligations may be subject to financial penalties representing 2% to 10% of the total value of the contract in question.

That rate may be increased to 4% to 20% in the event of a repeat infringement within five years of the date referred to in the first subparagraph of paragraph 8.

The institution shall determine the administrative or financial penalties taking into account in particular the elements referred to in Article 142(1) of the Regulation laying down the rules of application of the Financial Regulation.

5.2 Selection criteria

The following selection criteria will be used to select the tenderers.

If the tender is submitted by partners (as defined under section 2.2 above)

- the selection criteria in respect of financial and economic capacity (see point 5.2.2 below) are to be considered as setting minimum standards which must be fulfilled by each partner; consequently, documentary evidence has to be provided by each partner and an evaluation of the financial and economic capacity will be carried out for each of them;
- the selection criteria in respect of technical capacity (see 5.2.3 below) will be assessed in relation to the combined capacities of all the members of a partnership as a whole (including subcontractors)

Documentary evidence of the tenderers' claims in respect of the selection criteria is required as indicated below. The tender should also include any other document that the tenderer(s) wish(es) to include by way of clarification.

The tenderer may rely on the capacities of other entities, regardless of the legal nature of the links which it has with them. It must in that case prove to the Contracting Authority that it will have at its disposal the resources necessary for performance of the contract, for example by producing an undertaking on the part of those entities to place those resources at its disposal.

5.2.1 Professional information

Criterion 1:	Enrolment in one of the professional or trade registers in the country of establishment or equivalent
Documentary evidence:	Declaration or certificate of enrolment in one of the professional or trade registers in the country of establishment

5.2.2 Financial and economic capacity

Criterion 2:	Sufficient financial and economic standing to guarantee continuous and satisfactory performance throughout the envisaged lifetime of the contract
Documentary	Photocopies of annual income statements and balance sheets or extracts

evidence:	<p>there from signed by the authorised representative of the legal entity for the last two financial years, where applicable, as approved by the general assembly of the company, audited and/or published</p> <p>AND</p> <p>Statements of overall turnover and turnover from contracts in the field of Internet monitoring, cyber-censorship, human rights, freedom of expression, Internet security, tool development, software development or digital activism in the last two financial years.</p>
-----------	--

If, for some exceptional reason which the Commission considers justified, a tenderer is unable to provide one or other of the above documents, he or she may prove his or her economic and financial capacity by any other document which the Commission considers appropriate. In any case, **the Commission must at least be notified of the exceptional reason and its justification in the tender.** The Commission reserves the right to request any other document enabling it to verify the tenderer's economic and financial capacity.

5.2.3 Technical background

Criterion 3:	Relevant expertise of the tenderer and other applicants, including subcontractors if any, acquired in the last three years, in the field of Internet and events monitoring; Internet infrastructure monitoring and management; Internet security monitoring; Information security; Internet data collection and analysis; Open Source tool development; circumvention tools; Internet science research; human rights monitoring; monitoring of Internet/ICT legal and policy developments; journalistic and media monitoring; digital rights and activism; censorship; surveillance; crisis management and early warning; freedom of expression.
Documentary evidence:	List of 3 contracts in the fields listed above performed in the past three years, or currently being performed, with their respective values.

Criterion 4:	Experience, technical knowledge and credibility of proposed team
Documentary evidence:	<p>Concise but informative curricula vitae of team members, demonstrating professional experience, including the requisite language skills, in the field of Internet and events monitoring; Internet infrastructure monitoring and management; Internet security monitoring; Information security; Internet data collection and analysis; Open Source tool development; circumvention tools; Internet science research; human rights monitoring; monitoring of Internet/ICT legal and policy developments; journalistic and media monitoring; digital rights and activism; censorship; surveillance; crisis management and early warning; freedom of expression, of at least 3 years.</p> <p>The Europass curriculum vitae template (available at http://europass.cedefop.europa.eu/europass/home/hornav/Introduction.csp) shall be filled in by each person involved in the execution of the tasks foreseen in the tender. Please make sure the precise contractual link with</p>

	the tenderer is clearly indicated.
--	------------------------------------

Criterion 5:	Management capability
Documentary evidence:	List of 3 contracts of a value of at least 50 000 EUR (fifty thousand) each, performed by the tenderer(s) (including subcontractor(s), if any) in the last 2 years. ¹⁷ Short description of the measures employed to ensure the quality of the services for each of the listed contracts.

5.3 Award criteria

5.3.1 Technical award criteria

The tenders will be qualitatively assessed on the basis of the technical award criteria and respective scores listed below:

<u>Technical award criterion</u>	<u>Maximum score/weighting</u>	<u>Threshold</u>
I. Understanding of the tasks required I.1. Understanding of the context outlined in Section 1 I. 2. Understanding of specific and long-term objectives in Section 2 I. 3. Understanding of the tasks described in Section 2 I. 4. Value added in respect of information included in the tender specifications <i>(All the sub-criteria above are of equal relative importance)</i>	30	15

¹⁷

If the tenderer(s) or subcontractor(s) participated as a partner in a consortium, the total value of the contract should be mentioned along with the value corresponding to the work executed by the partner.

<p>II. Technical quality of the tender</p> <p>II. 1. Quality of the conceptual approach to each of the tasks of the study.</p> <p>II. 2. Completeness and full coverage of the scope of the tasks</p> <p>II. 3. Quality of the approach proposed for the consultation and workshop</p> <p>II. 4. Diversity of data sources, categories and aggregators</p> <p>II. 5. Degree of openness and interoperability of the proposed approach</p> <p>II. 6. Degree of innovation in the proposed approach</p> <p>II. 7. Degree of sustainability of the proposed approach</p> <p>II. 8. Value added at the EU level and use of available resources</p> <p>II. 9. Quality of the methodological approach /Methodology to collect and analyse data / Soundness and appropriateness of the proposed analysis tools and data gathering techniques</p> <p>II. 10. Quality of the roadmap for the proposed deliverables, , including the final data set for publication and data linking</p> <p>II. 11. Quality and extent of contacts proposed with relevant public and private stakeholders in the sphere of the tasks of the tender.</p> <p>II. 12. Relevance, quality and completeness of the information proposed to be used, and of the analysis proposed to be undertaken</p> <p><i>(All the sub-criteria above are of equal relative importance)</i></p>	<p>50</p>	<p>25</p>
---	------------------	------------------

III. Management	20	10
III. 1. Feasibility to meet the objectives specified in the tender specifications (outlined e.g. by a work plan or timetable) III. 2. Sound, realistic and proportional allocation of: <ul style="list-style-type: none"> – financial and – human resources, including allocation of expertise, roles and responsibilities III. 4. Realistic approach of the work plan or timetable III. 5. Quality and feasibility of the action plan <i>(All the sub-criteria above are of equal relative importance)</i>		
TOTAL	100	60

Minimum score per criterion (threshold):

Tenders scoring less than 50% of the maximum score for any technical award criterion will be considered of insufficient quality and rejected.

Minimum total score (threshold):

Tenders with a total score of less than 60 points at the end of the evaluation process will be considered of insufficient quality and rejected.

5.3.2 Price

The price quoted must comply with the requirements laid down in Part 2 - section 4.3 above.

6 AWARD OF THE CONTRACT

The Contract shall be awarded to the tender offering the best value for money, which will be the one with the best quality/price ratio, taking into account the award criteria listed in section 5.3.

The qualitative score obtained for the technical award criteria will be divided by the total price of the tender.

7 PAYMENT AND STANDARD CONTRACT

- Payments under the contract shall be made in accordance with articles I.4, I.10 and II.15 of the model contract attached, provided that the contractor has fulfilled all this contractual obligations.

The invoice shall be submitted in electronic format only by using the e-PRIOR communication platform. A brief description of the system and connection modalities is enclosed to the present Tender Specifications (Annex 8: e-PRIOR description). The tenderer(s) is/are required to inform the Commission about the

submission modality chosen for the dispatch of the invoice, should a contract be awarded to them. To this end, the tenderer should specify in Annex 9 (Cover letter for the tender) whether (s)he intends to use the Supplier Portal or establish a direct connection between the contractor's back office and the Commission's back-office/ use the services of a third party service provider already connected to e-PRIOR and offering such services.

Further instructions/guidance documents to assist contractors in sending electronic invoices will be communicated by the Commission after the contract award.

Contractors should note that since the model service contract for this call for tender foresees submission of electronic invoices, paper invoices will not be taken into account, except in the cases referred to in points 6 and 7 of Article I.10.2 (Submission and validity of financial documents) of the Model Service Contract attached.

8 VALIDITY OF THE TENDER

Period of validity of the tender shall be 9 months from the closing date for submission of the tender given above.

9 ADDITIONAL PROVISIONS

Changes to tenders will be accepted only if they are received on or before the final date set for the receipt of tenders.

Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.

No information of any kind will be given on the state of progress with regard to the evaluation of tenders.

All documents submitted by tenderers will become property of the Commission and will be regarded as confidential.

10 LIQUIDATED DAMAGES: SEE ARTICLE II.12 OF THE MODEL CONTRACT

11 NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on the Commission to award the contract. Should the invitation to tender cover several items or lots, the Commission reserves the right to award a contract for only some of them. The Commission shall not be liable for any compensation with respect to tenderers whose tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

12 RESULTS

The results of the service must be forwarded to the European Commission in Brussels. **The copyright will belong to the Commission;** the Commission will in particular have the right to publish the results, including the structured final data.

If the result is not to be fully created for the purpose of the contract it is to be clearly pointed out in the tender. There should be information provided about the scope of pre-existing materials, their source and when and how right to have them have been acquired.

The provisions on the use of the results and ownership of the results can be found in the Model Service Contract (Article I.8 Exploitation of the results of the contract and Article II.10 Ownership of the results – Intellectual and Industrial Property Rights).

PART 3: ANNEXES

ANNEX 1: ADMINISTRATIVE IDENTIFICATION FORM

European Capability for Situational Awareness – SMART 2013/N004

<u>TENDERER'S ID</u>	
Name	
Legal form	
Date of registration	
Country of registration	
Registration number	
VAT number	
Address of registered office	
Contact address (if different)	
URL	
<u>AUTHORISED REPRESENTATIVE(S)¹⁸</u>	
<u>CONTACT PERSON</u>	
Name	
Forename	
Position	
Telephone	
Fax	
Email	

¹ Please include the names of the legal representative(s) whose contract signature is required in accordance with the statutes of the organisation and the official document to be provided as required in Part 2 under section 2.3

<p>DECLARATION BY THE AUTHORISED REPRESENTATIVE(S): I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.</p>

Place and date:

Name (in capital letters) and signature:

ANNEX 2: LEGAL ENTITIES FORM

As required in PART 2 under section 2.3 of the tender specifications.

A standard template in each EU language is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

ANNEX 3: BANK IDENTIFICATION FORM

As required in PART 2 under section 2.3 of the tender specifications

A standard template in each EU language is available at:

http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm

<p style="text-align: center;">ANNEX 4: DECLARATION OF HONOUR ON EXCLUSION CRITERIA AND ABSENCE OF CONFLICT OF INTEREST</p>
--

European Capability for Situational Awareness – SMART 2013/N004

(Complete or delete the parts in blue italics in parentheses)

[Choose options for parts in blue between square brackets]

The undersigned *(insert name of the signatory of this form)*:

in [his][her] own name *(for a natural person)*

or

representing the following legal person: *(only if the economic operator is a legal person)*

full official name:

official legal form:

full official address:

VAT registration number:

- declares that [the above-mentioned legal person][he][she] is not in one of the following situations:
- a) is bankrupt or being wound up, is having its affairs administered by the courts, has entered into an arrangement with creditors, has suspended business activities, is the subject of proceedings concerning those matters, or is in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
 - b) has been convicted of an offence concerning professional conduct by a judgment of a competent authority of a Member State which has the force of *res judicata*;
 - c) has been guilty of grave professional misconduct proven by any means which the contracting authorities can justify including by decisions of the European Investment Bank and international organisations;
 - d) is not in compliance with all its obligations relating to the payment of social security contributions and the payment of taxes in accordance with the legal provisions of the country in which it is established, with those of the country of the contracting authority and those of the country where the contract is to be performed;
 - e) has been the subject of a judgement which has the force of *res judicata* for fraud, corruption, involvement in a criminal organisation, money laundering or any other illegal activity, where such activity is detrimental to the Union's financial interests;
 - f) is a subject of an administrative penalty for being guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in a procurement procedure or failing to supply this information, or having been declared to be in serious breach of its obligations under contracts covered by the Union's budget.
- *(Only for legal persons other than Member States and local authorities, otherwise delete)* declares that the natural persons with power of representation, decision-

making or control¹⁹ over the above-mentioned legal entity are not in the situations referred to in b) and e) above;

- declares that [the above-mentioned legal person][he][she]:has no conflict of interest in connection with the contract; a conflict of interest could arise in particular as a result of economic interests, political or national affinity, family, emotional life or any other shared interest;
 - h) will inform the contracting authority, without delay, of any situation considered a conflict of interest or which could give rise to a conflict of interest;
 - i) has not granted and will not grant, has not sought and will not seek, has not attempted and will not attempt to obtain, and has not accepted and will not accept any advantage, financial or in kind, to or from any party whatsoever, where such advantage constitutes an illegal practice or involves corruption, either directly or indirectly, inasmuch as it is an incentive or reward relating to award of the contract;
 - j) provided accurate, sincere and complete information to the contracting authority within the context of this procurement procedure ;
- acknowledges that [the above-mentioned legal person][he][she] may be subject to administrative and financial penalties²⁰ if any of the declarations or information provided prove to be false.

In case of award of contract, the following evidence shall be provided upon request and within the time limit set by the contracting authority:

For situations described in (a), (b) and (e), production of a recent extract from the judicial record is required or, failing that, a recent equivalent document issued by a judicial or administrative authority in the country of origin or provenance showing that those requirements are satisfied. Where the tenderer is a legal person and the national legislation of the country in which the tenderer is established does not allow the provision of such documents for legal persons, the documents should be provided for natural persons, such as the company directors or any person with powers of representation, decision making or control in relation to the tenderer.

For the situation described in point (d) above, recent certificates or letters issued by the competent authorities of the State concerned are required. These documents must provide evidence covering all taxes and social security contributions for which the tenderer is liable, including for example, VAT, income tax (natural persons only), company tax (legal persons only) and social security contributions.

For any of the situations (a), (b), (d) or (e), where any document described in two paragraphs above is not issued in the country concerned, it may be replaced by a sworn or, failing that, a solemn statement

19

¹ This covers the company directors, members of the management or supervisory bodies, and cases where one natural person holds a majority of shares.

20

¹ As provided for in Article 109 of the Financial Regulation (EU, Euratom) 966/2012 and Article 145 of the Rules of Application of the Financial Regulation

made by the interested party before a judicial or administrative authority, a notary or a qualified professional body in his country of origin or provenance.

If the tenderer is a legal person, information on the natural persons with power of representation, decision making or control over the legal person shall be provided only upon request by the contracting authority.

Full name

Date

Signature

ANNEX 5: POWER OF ATTORNEY²¹

MANDATING ONE OF THE PARTNERS IN A JOINT TENDER AS LEAD
PARTNER AND LEAD CONTRACTOR
European Capability for Situational Awareness – SMART 2013/N004

21

¹ To be filled in and signed by each of the partners in a joint tender, except the lead partner;

The undersigned:

– Signatory (Name, Function, Company, Registered address, VAT Number)

having the legal capacity required to act on behalf of his/her company,

HEREBY AGREES TO THE FOLLOWING:

1. To submit a tender as a partner in the group of partners constituted by Company 1, Company 2, Company N, and led by Company X, in accordance with the conditions specified in the tender specifications and the terms specified in the tender to which this power of attorney is attached.
2. If the European Commission awards the Contract to the group of partners constituted by Company 1, Company 2, Company N, and led by Company X on the basis of the joint tender to which this power of attorney is attached, all the partners shall be co-signatories of the Contract in accordance with the following conditions:
 - (a) All partners shall be jointly and severally liable towards the European Commission for the performance of the Contract.
 - (b) All partners shall comply with the terms and conditions of the Contract and ensure the proper delivery of their respective share of the services and/or supplies subject to the Contract.
 - 1) Payments by the European Commission related to the services and/or supplies subject to the Contract shall be made through the lead partner's bank account: [Provide details on bank, address, account number].
 - 2) The partners grant to the lead partner all the necessary powers to act on their behalf in the submission of the tender and conclusion of the Contract, including:
 - (a) The lead partner shall submit the tender on behalf of the group of partners.
 - (b) The lead partner shall sign any contractual documents — including the Contract, and Amendments thereto — and issue any invoices related to the Services on behalf of the group of partners.
 - (c) The lead partner shall act as a single contact point with the European Commission in the delivery of the services and/or supplies subject to the Contract. It shall co-ordinate the delivery of the services and/or supplies by the group of partners to the European Commission, and shall see to a proper administration of the Contract.

Any modification to the present power of attorney shall be subject to the European Commission's express approval. This power of attorney shall expire when all the contractual obligations of the group of partners towards the European Commission for the delivery of the services and/or supplies subject to the Contract have ceased to exist. The parties cannot terminate it before that date without the Commission's consent.

Signed in on [dd/mm/yyyy]

Place and date:

Name (in capital letters), function, company and signature:

ANNEX 6A: LETTER OF INTENT FOR SUB-CONTRACTORS

European Capability for Situational Awareness – SMART 2013/N004

The undersigned:

.....

Name of the company/organisation:

.....

Address:

.....

Declares hereby that, in case the contract is awarded to [name of the tenderer], the company/organisation that he/she represents, intends to collaborate in the execution of the tasks subject to this call for tender, in accordance with the tender specifications and the tender to which the present form is annexed, and is available to carry out its part of the tasks during the period foreseen for the execution of the contract.

Declares hereby taking note of Art. II.7 regarding subcontracting and Art. II.18 in relation with checks and audits of the service contract.

Place and date:

Name (in capital letters) and signature:

ANNEX 6B: LETTER OF INTENT FOR EXTERNAL EXPERTS

European Capability for Situational Awareness – SMART 2013/N004

The undersigned:

.....

Address:

.....

Declares hereby that, in case the contract is awarded to [name of the tenderer], he/she intends to collaborate in an individual capacity as **an external expert** in the execution of the tasks subject to this call for tender, in accordance with the tender specifications and the tender to which the present form is annexed, and is available to carry out its part of the tasks during the period foreseen for the execution of the contract. In addition, the undersigned declares not to have any conflict of interest in connection with the contract, and not to be in one of the situations of exclusion referred to in Article 106(1) of the Financial Regulation²².

Declares hereby taking note of Art. II.7 regarding subcontracting and Art. II.18 in relation with checks and audits of the service contract.

Place and date:

Name (in capital letters) and signature:

22

¹ Available at http://ec.europa.eu/budget/documents/financial_regulation_en.htm

ANNEX 7: CHECK LIST OF DOCUMENTS TO BE SUBMITTED

European Capability for Situational Awareness – SMART 2013/N004

The purpose of the table below is to facilitate the preparation of the tender by providing an overview of the documents that must be included (marked by ■) depending on the role of each economic operator in the tender (be it lead partner, partner in joint bid, single tenderer or subcontractor/external expert). Some of the documents are only relevant in cases of joint bids or when subcontractors are involved. Additional documents might be necessary depending on the specific characteristics of each tender.

Description	L e a d p a r t n e r i n a j o i n t b i d	All the other partners in a joint bid	Single tenderer (with or without subcontractors)	Subcontractor	Subcontractor – External expert
<i>Administrative section of the tender</i>					
Annex 1: Original Administrative identification form (see section 2.3, part 2)	■	■	■	■	

Annex 2: Original Legal Entity Form (see section 2.3, part 2)	■	■	■		
Annex 3: Original Financial Identification form (see section 2.3, part 2)	■		■		
Annex 4: Original Declaration of honour with respect to the Exclusion Criteria and absence of conflict of interest (see section 2.3, part 2)	■	■	■	■	
Annex 5: Original Power of attorney (see section 2.3, part 2)		■			
Annex 6 a: Original Letter of intent from each subcontractor (see section 2.3, part 2)				■	
Annex 6 b: Original Letter of intent from each subcontractor (see section 2.3, part 2)					■
Annex 9: Cover letter for the tender	■		■		
Legible photocopy of the statutes of the entity (see section 2.3, part 2)	■	■	■		
Legible photocopy of the notice of appointment of the persons authorised to represent the tenderer (see section 2.3, part 2)	■	■	■		
Declaration or certificate of enrolment in one of the professional or trade registers in the country of establishment (see section 5.2.1, part 2)	■	■	■		
Evidence of financial and economic capacity (see section 5.2.2, part 2)	■	■	■		
Evidence of Technical background (see section 5.2.3, part 2)	■	■	■	■	■
<i>Technical Section of the tender (see section 4.2, part 2)</i>	■		■		
<i>Financial Section of the tender (see section 4.3, part 2)</i>	■		■		

ANNEX 8: E-PRIOR DESCRIPTION

1.1. What is e-PRIOR

e-PRIOR is the service-oriented communication platform²³ that allows electronic procurement (e-Procurement) between suppliers and customers, targeted to the European Institutions, including the European Commission.

e-Procurement consists in exchanging procurement documents such as Requests, Offers, Orders, Catalogues, Invoices, etc. in an electronic format following standards. The standards that are used by e-PRIOR are promoted by the CEN ("Comité Européen de Normalisation"). Using standards allows the interoperability between the IT systems (back-offices) of the suppliers on one hand and those of the customers on the other hand.

1.2. e-PRIOR Ways of communication

There are two main ways for communicating/exchanging electronic documents between the suppliers/contractors and the European Institutions:

- Through a direct connection between the supplier's back-office and the Commission/contracting authority's back-office, via interfaces using secured web-services (machine-to-machine communication). In this case the suppliers have the option to:
 - Develop themselves the connection to e-PRIOR or,
 - Pass through a third party Service Provider already connected to e-PRIOR and offering such services²⁴.
- Via Web Portals - Supplier and Customer portal - where specific user interfaces running in an Internet Browser may be used by end-user to create and manage electronic documents such as receiving and approving orders, creating electronic invoices²⁵ and receiving acknowledgements, sending dispatch advices and receipt advices.

23

¹ For more information please consult http://ec.europa.eu/dgs/informatics/supplier_portal/index_en.htm

24

¹ Service providers already connected to e-PRIOR: AdValvas, b2boost, certipost, inovis.

25

¹ The User's manual for e-invoicing on the Supplier Portal is available for consultation at http://ec.europa.eu/dgs/informatics/supplier_portal/documentation/documentation_en.htm

Both communication ways may be used simultaneously and combined together. Nevertheless, the machine-to-machine communication is targeted for suppliers managing large number of documents (>100 invoices/orders/etc. per year), whereas the Supplier Portal is mainly used by suppliers, such as SME's or individuals, managing few documents per year. In case of connection via web services, Directorate-General for Informatics (DIGIT) will provide all the necessary assistance.

1.3. e-PRIOR Modules

e-PRIOR is made up of several modules, but only the e-Invoicing module (standard invoices and credit notes) will be used in the execution of this contract.

1.4. What is the added value of e-PRIOR?

- Paperless
 - Reduced encoding/transaction costs
 - Faster communication
 - Reduced payment delays
 - Secure and transparent processes
 - Environmental friendly
-

ANNEX 9: COVER LETTER FOR THE TENDER

Please select the appropriate option

OPTION 1

Single legal person or private/ public entity

- The offer is submitted by a **one tenderer**.

OPTION 2

Joint offers

- The offer is submitted by **partners**.
 - Company acting as **lead partner** for the group of tenderers:
.....
 - **Other partners** taking part in the joint tender:
.....
.....

OPTION 3

Joint offers

- The offer is submitted by one tenderer **with subcontractors**.
 - Company acting as **tenderer**:
.....
 - **Subcontractors**:
.....
.....

OPTION 4

Joint offers

The offer is submitted by partners **with subcontractors**.

- Company acting as **lead partner** for the group of tenderers:

.....

- **Other partners** taking part in the joint tender:

.....

.....

- **Subcontractors:**

.....

.....

Submission modality for the dispatch of the invoice

Via the Supplier Portal

Via a direct connection

Between the Contractor's back office and the Commission's back office

Using the services of a third party service provider already connected to e-PRIOR and offering such services

- Name of the third party service provider:

.....

ANNEX 10: TEMPLATE STUDY FINAL REPORT OR EXECUTIVE SUMMARY



B Title

C Subtitle (optional)

D Insert cover picture here (optional)

F This study was carried out for the European Commission by

G Logo(s) + Company identifier(s) + Authors' name(s) (optional)

H

Internal identification

Contract number:

SMART number

European Commission

L Title

Luxembourg, Publications Office of the European Union

M xxxx – number of pages

N

ISBN number
DOI: number



Q

LEGEND:

This template – which respects the Visual Identity of the Commission and incorporates the OP identifiers – is the recommended layout for DG CONNECT studies. Modifications are possible but should be limited (contact Unit F4 if needed).

Front cover

- A: - The banner on the top of the cover page can be of a different colour although for the Digital Agenda related publication blue colour is preferred.
- The line under the Commission logo has to be of the same colour of the F element.
- B-C-D: Font is Verdana. Size can be adapted appropriately to the length of the title / subtitle.
The size of the picture can vary. If no picture, don't center the title over the page.
- E: Choose between "Final Report" or "Executive Summary"
- F: If (exceptionally) the study is not related to the area policy of the Digital Agenda another policy can be indicated or "DG CONNECT" can be written in box F.

Inside front cover

- G: Authors' name(s) are optional
- H: Contract number and SMART number (if available)
- I: See O, P
- J: Replace XXXX with the year of publication
- K: The clause can only be inserted if the following conditions are fulfilled:
- No third-party textual or artistic material is included in the publication without the Copyright holder's prior consent to further dissemination and reuse by other third parties or:
 - An additional notice specifies that the reproduction of the third-party textual or artistic material included in the study is prohibited

Inside back cover

- L: Title of the publication
- M: Replace XXXX with the year of publication and write the total amount of pages
- N: See O, P

Back cover

- O, P: ISBN, DOI (Digital Object Identifier), Catalogue Number
These three identifiers are mandatory on each Final Report and on each Executive Summary (each language version has separate identifiers). They must be obtained from the OP before the publication. Non-public Final Reports and/or Executive Summaries receive only a catalogue number.
- O: This banner has to have the same colour of banner A
- Q: No text on this page. Only background .