TERMS OF REFERENCE

Impact Assessment of possible measures to enhance cooperation, coordination and information exchange in the area of Internet security between Member States and stakeholders, including across sectors, in the EU

SMART 2012/0002

Under the Framework Contract No SMART 2007/0035 – Lot 2: "Provision of Impact Assessment Tasks in the Sphere of Regulation on the Electronic Communications Sector"

TABLE OF CONTENTS

PART 1: TECHNICAL DESCRIPTION

1 CONTEXT, POLICY BACKGROUND AND PROBLEM DEFINITION

1.1 Context

Over the last decade, the Internet has become the nervous system of our economy and society as a whole.

At the same time, we are witnessing that the threat landscape is constantly expanding and the number and seriousness of attacks is increasing Internet's vulnerability. Such threats can now originate from anywhere in the world and, due to global interconnectedness, impact any other part of the world. According to the World Economic Forum there is a 10% likelihood of a major Critical information infrastructure breakdown with potential economic damages of over $ 250 billion.

Securing the smooth functioning of this vital infrastructure is therefore essential to our economic stability and growth. Failure to do so, would pose an enormous risk to the proper functioning of the single market in terms of lost growth, jobs and prosperity, and to reaching our goal of achieving a true digital single market by 2015.

It is therefore crucial that the EU recognises the need for an effective European Strategy for Internet Security to avert and/or minimise the risk of a major attack or technical failure of its information and communication infrastructures.

1.2 Policy background

In 2006, a Strategy for a Secure Information Society[1] was adopted in response to the urgent need to coordinate efforts for building up trust and confidence of stakeholders in electronic communications and services. The main elements of this strategy were endorsed in a Council Resolution[2]. This strategy also strengthened the role of the European Network and Information Security Agency (ENISA), established in 2004 with a view to contribute to the goals of ensuring a high and effective level of network and information security (NIS) within the Union and to develop a culture of NIS for the benefit of EU citizens, consumers, enterprises and public sector organisations in the EU.

On 30 March 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP)[3] focusing on the protection of Europe from cyber attacks and cyber disruptions by enhancing preparedness, security and resilience. The Communication launched an action plan with five pillars of actions: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector.

The Action plan was endorsed in the Presidency Conclusions of the Ministerial Conference on CIIP in Tallinn in 2009[4]. These commitments were further advanced by the Council

[1] COM(2006)251
[2] 2007/068/01
[3] COM(2009)149
[4] http://www.riso.ee/tallinnciip/
http://www.riso.ee/tallinnciip/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf

Resolution on "A collaborative European approach to network and information security" adopted on 18 December 2009[5].

Security and resilience issues are notably addressed under the Trust and Security chapter of the Digital Agenda for Europe (DAE)[6], one of the flagship initiatives of the EU 2020 Strategy. In particular, its Key action 6 calls for measures aimed at a reinforced and high level Network and Information Security policy.

The DAE is complementary to other initiatives such as the Stockholm Programme for Freedom, Security and Justice and the Internal Security Strategy in action[7].

More recently, two key policy components have been completing this picture, from the network and information security angle:

- The activity of the European Network and Information Security Agency (ENISA), for which a proposal to modernise the mandate is under discussion in the Council and the European Parliament[8];

- The Commission second Communication on CIIP of March 2011[9] ('Achievements and next steps: towards global cyber-security') which takes stock of the results achieved since the adoption of the CIIP action plan in 2009 and describes the next priorities planned under each action at both European and international level. Council Conclusions on CIIP were adopted on 27 May 2011.

The revised regulatory framework for electronic communications also sets new security provisions, including security breaches notifications obligation (Art. 13a and 13b), to be transposed at national level by 25 May 2011.

Discussions are also ongoing in the European Parliament and the Council as regards relevant proposals on a Directive on attacks against information systems and on a Directive on combating sexual abuse, sexual exploitation of children and child pornography.

International cooperation is also a key priority in this area. In particular:

- The DAE calls for working with global stakeholders notably to strengthen global risk management;

- In its second Communication on CIIP of March 2011, the Commission committed to promote a culture of global risk management by promoting internationally the European principles and guidelines for the resilience and stability of the Internet[10], building strategic international partnerships and developing trust in the cloud.

A key step in this regard has been the establishment, since the 2010 EU-US Summit, of a EU-US Working Group on Cyber-security and Cyber-crime.

[5] Doc 15841/09
[6] COM(2010)245
[7] COM(2010)673
[8] COM(2010)521
[9] COM(2011) 163
[10] http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf

1.3 Problem definition

Despite the progress made so far under the various EU initiatives listed above, the cyber-security capabilities within the EU are still not at the level which is necessary in order to ensure a high and efficient protection within the EU and to keep pace with the fast-changing threat landscape.

There is a need for a step change in the way Internet security issues are approached in the EU. To this end, the Commission will propose in 2012 a comprehensive European Strategy for Internet Security, with the overall policy objective to put in place a robust line of defence against cyber disruptions and attacks.

The increasing sophistication of threats and the global interconnectedness call for a much tighter cooperation and collaboration between Governments, as well as between public and private sectors. There is an increasing need to put in place appropriate coordinating mechanisms and structures at national level, which would help ensure better cooperation and coordination at EU level amongst competent national authorities, as well as with the private sector, in cooperation with and benefiting from the support of relevant EU institutions, agencies and bodies. Such mechanisms should stimulate more efficient information exchange and lead to improved governance in the area of Internet security at EU level, thereby contributing to the smooth functioning of the internal market.

2 OBJECTIVES

The ***main objective*** of the study is to provide assistance in shaping and assessing policy options for measures to enhance cooperation, coordination and information exchange in the area of Internet security, both on the prevention and response sides, between Member States and stakeholders, including across sectors, with a view to ensure the well-functioning of the internal market.

The *tenderer* shall propose a limited set of possible options (maximum 5) ranging from "business as usual" to soft measures and strong regulatory instruments which could be put in place in order to ensure that:

– There are clear roles and responsibilities of MS and the EU as well as coordination and cooperation mechanisms (political, strategic and operational ones) at EU level to prevent, detect, mitigate and respond to cyber incidents/disruptions (e.g. defined in a European cyber incident contingency plan that could be agreed as a political document);

– Computer Emergency Response Teams (CERTs) and bodies competent for Internet security (competent bodies) in the Member States are part of an effective network at EU level in which relevant information is exchanged in accordance with standards of confidentiality;

– Each Member State has in place a well-functioning body at technical level (CERT) to detect, prevent, respond to attacks and disruptions to the proper functioning of the Internet;

– The private sector has a general obligation to notify security breaches to competent bodies, as challenges are common and early warning and shared solutions are needed. This could also be accompanied by mandatory security audits and authorisation mechanisms where this is already required by applicable law (e.g. energy, banking).

– There is not only efficient EU-wide but also International cooperation, as interdependencies are cross-border and Internet security issues have a global nature.

The tenderer shall also examine existing cooperation models used in other sectors such as health and consumer protection, financial services, energy, where steps have been taken to ensure effective cooperation and coordination between Member States' competent authorities, and where relevant, the private sector.

Specific objectives:

– Understanding and analysing the current situation in the EU, the barriers to efficient cooperation, coordination and exchange of information on Internet security threats and disruptions at EU-level;

– Analysing measures adopted at EU level in other sectors such as health, financial services and energy to set up cooperation mechanisms and processes to ensure the well-functioning of the internal market and drawing best practices which could be applied in the area of Internet security;

– Outlining proposals for policy options as mentioned above;

– Refining the policy options and accompanying measures in agreement with the Commission services;

– Cost/benefit analysis of potential impacts of the short-listed policy options in economic, social and environmental terms according to the Commission practice described in the Impact Assessment Guidelines[11].

3 DURATION

Duration of the tasks must not exceed 4 months and is subject to the provisions of Article I.2.3 of the Framework Contract.

4 DELIVERABLES, MEETINGS AND TIMETABLE

4.1 Deliverables

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

- **D1: Inception report.** The report should include an overview of the analysis of the current situation and an initial description of the policy options and accompanying measures, reflecting the discussions with the Commission. The Inception Report shall be made available within 1 week after the kick-off meeting.

- **D2: Interim study report.** The report should provide a detailed description of the examined policy options and contain an initial assessment of the nature of their impacts. The interim study report shall be made available to the Commission's services within 5 weeks after signature of the contract by the last contracting party and will be presented by the Contractor at the interim meeting.

[11] http://ec.europa.eu/governance/impact/commission_guidelines/commission_guidelines_en.htm

- **D3: Draft final study report.** The content of the draft final report should be structured in line with the requirements for the final report (see D4). It shall be made available to the Commission's services within 9 weeks after signature of the contract by the last contracting party.

- **D4: Final study report**, including the following sections:

    1. **Executive summary** (not more than 1 page, written in non-technical language, presenting the conclusions from the comparison of the short-listed policy options)
    2. **Section 1:** Methodology (summary of the methodology used to yield the study results)
    3. **Section 2:** Problem definition
    4. **Section 3:** Objectives
    5. **Section 4:** Policy options
    6. **Section 5:** Analysis of impacts
    7. **Section 6:** Comparison of the options
    8. **Section 7:** Conclusions
    9. **Annexes** containing any factual or technical material.

The final study report shall be made available to the Commission's services within 11 weeks after signature of the contract by the last contracting party.

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 5 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.

4.2 Meetings

The following meetings will be held during the study:

1) A **kick-off meeting** will be organised by the Commission's services at the Commission's premises in Brussels within 1 week after signature of the contract to discuss the priorities for the study and refine the Contractor's workplan. The Commission and the Contractor will discuss and agree on which options should be

analysed at the next stage by the contractor. Within a week from the kick-off meeting the Contractor will establish a brief inception report, together with the minutes of the meeting. This should reflect the understanding of the subject and serve as a guide to the work conducted during the lifetime of the project.

2) A **second meeting** during which the contractor will present the interim findings will be held within 6 weeks after signature of the contract. The Contractor shall provide a detailed description of the examined policy options and present the initial assessment of the nature of their impacts.

3) A **final meeting** during which the contractor will present the final findings and proposed conclusions will be held within 10 weeks after signature of the contract. The contractor will have to finalise the final study report on the basis of the outcome of the final meeting.

The above meetings will be organised by DG Information Society and Media services at its premises in Brussels. The Contractor will bear the costs of attendance of its own staff for all of the above meetings.

4.3 Timetable

Deliverable ↓	**Meeting** ↓	**Month** →	1	2	3	4
		Week ↓				
	Kick-off meeting	0 + 1				
D1: Inception report		0 + 2				
D2: Interim study report		0 + 5				
	Interim meeting	0 + 6				
D3: Draft final study report		0 + 9				
	Final meeting	0 + 10				
D4: Final study Report		0 + 11				

5 TERMS OF APPROVAL OF REPORTS

After reception of each study report included in section 4.1 above, the Commission will have 20 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 15 calendar days. The new report shall likewise be subject to the above provisions.

PART 2: ADMINISTRATIVE DETAILS

1 ELIGIBILITY REQUIREMENTS

All the **requirements** related to the **submission and opening of the tenders** are detailed in the request for services including:

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

2 SPECIFIC TENDER PRESENTATION

The specific tender for the tasks required under the specific contract has to include an outline of the methodologies proposed, a work programme, a budget table containing allocation of human resources to be spent, and a lump-sum price for the order, based on the price schedule defined under point 10.3 of the Tender Specifications of the Framework contract. More specifically:

– The tender must be signed by the tenderer or his duly authorised representative.

– The tender must be in conformity with the framework contract and must include:

  – The total amount in EUR (€) payable for the services that are the subject of this request, broken down by categories of experts, travel and mission expenses (see point 5. here below);

  – A detailed description of the proposed work to be undertaken, which develops further the evaluation questions and links them to the tasks with sound methodologies;

  – An outline of the methodologies proposed together with a detailed description of each methodology, how it will be undertaken, how it will be brought to a successful conclusion etc;

  – A work-plan and timetable, including a clear description of the management structure;

  – The composition of the proposed team: names, categories of expertise, CVs and the number of man-days to be supplied for each expert;

  – The proposed assignment of the proposed experts as well as the allocation of other resources to tasks;

  – A statement on the absence of conflict of interest.

The conditions for the work are specified in the accompanying draft Specific Contract.

3 AWARD CRITERIA

In accordance with the indications of Annex II to the Tender Specifications of the framework contract No. CE 30-0205088/00-06, the evaluation committee will evaluate the tenders and select the actual contractor based on the following 3 overall award criteria, each of which is weighted as shown below. Sub-criteria listed under each overall criterion are of equal value.

1)	**Understanding of the services and general approach and work to be performed** *i)* Understanding of the domain of Network and Information Security *ii)* Understanding of the task in relation to the Commission's impact assessment requirements and quality criteria *iii)* Understanding of impact assessment and cost-benefit analysis techniques *(The above aspects are of the same relative value)*	30 points
2)	**Proposed methodology and tools** *i)* Soundness and rigour of the proposed approach *ii)* Quality of methodology to identify broader impacts of policy options including economic effects *iii)* Completeness of the methodology including specification of how benefits – both tangible and intangible – will be measured *iv)* Quality of the cost-benefit analysis including specification of methods *(The above aspects are of the same relative value)*	50 points
3)	**Approach proposed for the management of the work** *i)* Soundness of resources and expertise allocation *ii)* Work plan and organisation of work; ability to deliver under tight deadlines *iii)* Verifiable objectives *iv*) Balanced and consistent method of work *(The above aspects are of the same relative value)*	20 points

Tenders which do not obtain at least 50% of the maximum score for each award criterion and at least 60% of the overall total score will be rejected.

In accordance with the indications of Annex II to the Tender Specifications of the framework contract No. CE 30-0205088/00-06, the tenders will be assessed in terms of the total price for the tender on the basis of the specific unit prices set in the Framework contract, broken down by categories of experts and travel and mission expenses.

The specific contract will be awarded to the most economically advantageous tender. This will be determined on the basis of the price to quality ratio of the tender and the bid with the best price/quality ratio will be selected for award.

4 PAYMENT AND STANDARD CONTRACT

Payments under the contract shall be made in accordance with article III.4 of the model specific contract attached and the relevant provisions of the Framework Contract.

5 PRICE

The maximum budget for the services to be provided under the specific contract is EUR 200 000 (two hundred thousand Euros). Offers above this amount will not be considered for evaluation.

A total fixed price expressed in EUR shall be included in the offer in accordance with the financial section of the Tender Specifications of the Framework Contract. The contract prices shall be firm and not subject to revision.

The price quoted must **be exclusive of all taxes**:

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).

A total fixed price expressed in EUR, which shall be broken down into:

A) Fees for personnel: fees determined in accordance with the Price Schedule submitted with the tender and annexed to the Framework Contract. The price offer should be based on the terms of reference of the specific contract.

B) Travel and subsistence cost: costs of all travel & subsistence costs considered necessary for the execution of the tasks of the specific contract according to the terms of reference. Contractors must also indicate how many travels are planned and to what destinations. The travel and subsistence costs will be paid as a lump-sum as part of the total price of the specific contract.

The total fixed price (A+B) will be used to calculate the quality/price ratio in order to determine the economically most advantageous offer for each specific request for services.

Under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities of 8 April 1965 (OJ L 152 of 13 July 1967), the Communities are exempt from all charges, taxes and dues, including value added tax; such charges may not therefore be included in the calculation of the price quoted; **the VAT amount must be indicated separately**. 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.

Prices shall be subject to the terms set in Article I.3 of the draft specific contract attached. The type of costs included in each price offer must fall within the scope of each specific request for services and terms of reference.

The part of each specific contract that the tenderer intends to subcontract shall be precisely indicated and detailed.

6 CONFIDENTIALITY

All non-published materials given to the contractor by DG Information Society and Media or other services of the European Commission are strictly confidential. The contractor will not allow information to be divulged to other parties or entities unless permission has been given by the Commission.

7 VALIDITY OF THE OFFER

Six months from the deadline for the submission of proposals.

8 DISCLAIMER

The following phrase is to be prominently displayed on the cover of all reports and deliverables:

"The opinions expressed in this report are those of the authors and do not necessarily reflect the views of the European Commission."