



OPEN CALL FOR TENDERS

Tender Specifications

“Reinforcing operational aspects of national / governmental CERTs”

ENISA P/35/10/TCD

LOT 1 - Operational gaps and overlaps on European level;

LOT 2 - Proactive detection of network security incidents;

LOT 3 - Secure communication with the CERTs and other stakeholders;

- Part 1** **Introduction**
- Part 2** **Technical Description**
- Part 3** **Administrative Details**

Annex I	Legal Entity Form
Annex II	Financial Identification Form
Annex III	Declaration of Honour for exclusion criteria & absence of conflict of interest
Annex IV	Financial Offer form
Annex V	Draft Service contract
Annex VI	Declaration by Authorised Representative
Annex VII	Consortium Form
Annex VIII	Sub-Contractors Form
Annex IX	Document Checklist

CONTENTS

PART 1 INTRODUCTION TO ENISA	5
1. BACKGROUND	5
2. SCOPE.....	5
3. OBJECTIVES.....	5
4. TASKS	6
5. ORGANISATIONAL FRAMEWORK.....	6
6. ADDITIONAL INFORMATION.....	6
PART 2 TECHNICAL DESCRIPTION	7
A. THE PROGRAMME	7
B. SCOPE OF THIS TENDER	8
1 LOT 1: OPERATIONAL GAPS AND OVERLAPS ON EUROPEAN LEVEL	9
1.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES.....	9
1.2 OBJECTIVES AND TASKS.....	10
1.2.1 TASK 1: Analysis of services	10
1.2.2 TASK 2: Defining areas and activities where gaps or overlaps exist	11
1.2.3 TASK 3: Deriving concrete suggestions for ENISA.....	11
1.2.4 TASK 4: Presentation of the results	11
1.3 EXPECTED SKILLS.....	11
1.4 DURATION	12
1.5 DELIVERABLES	12
1.6 DURATION OF THE SERVICE.....	12
1.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS	12
1.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE	13
1.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER	13
2. LOT 2 - PROACTIVE DETECTION OF NETWORK SECURITY INCIDENTS	15
2.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES.....	15
2.2 OBJECTIVES AND TASKS.....	15
2.2.1 TASK 1: Desktop research of the existing measures.....	16
2.2.2 TASK 2: Survey of CERTs in Europe.....	16
2.2.3 TASK 3: Establishing expert group, initiating, moderating discussions.....	16
2.2.4 TASK 4: Analysis of the measures identified	16
2.2.5 TASK 5: Presentation of the results	17
2.3 EXPECTED SKILLS.....	17
2.4 DURATION	17
2.5 DELIVERABLES	18
2.6 DURATION OF THE SERVICE.....	18
2.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS	18
2.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE	18
2.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER	19
3. LOT 3 - SECURE COMMUNICATION WITH THE CERTs & OTHER STAKEHOLDERS	20
3.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES.....	20
3.2 OBJECTIVES AND TASKS.....	20
3.2.1 TASK 1: Stock taking of existing solutions.....	20
3.2.2 TASK 2: Analysis of the requirements	21
3.2.3 TASK 3: Provide a practical guide/roadmap for a suitable channel to start with	21
3.2.4 TASK 4: Project management	21

3.2.5	TASK 5: Presentation of the results	21
3.3	EXPECTED SKILLS.....	21
3.4	DURATION	22
3.5	DELIVERABLES	22
3.6	DURATION OF THE SERVICE.....	22
3.7	PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS	22
3.8	TENDER RESULT AND ESTIMATED CONTRACT VALUE	22
3.9	CONTENT AND PRESENTATION OF THE TECHNICAL OFFER	23
4.	CONTENT AND PRESENTATION OF THE PRICE OFFER.....	24
5.	PRICE	24
6.	PRICE REVISION	24
7.	COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER.....	24
8.	PERIOD OF VALIDITY OF THE TENDER	24
9.	PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES	24
10.	PAYMENT ARRANGEMENTS.....	24
11.	CONTRACTUAL DETAILS.....	24
PART 3	ADMINISTRATIVE DETAILS	25
1.	FORMAL REQUIREMENTS.....	25
1.1	Address and deadline for submission of the Tender:	25
1.2	Presentation of the Offer and Packaging.....	26
1.3	Identification of the Tenderer.....	26
1.4	Participation of consortia	28
1.5	Subcontracting	28
1.4	Signatures of the Tender	29
1.5	Total fixed price	29
1.6	Language	29
1.7	Opening of the Tenders.....	29
2.	GROUND FOR EXCLUSION OF TENDERERS	29
2.1	Reasons for Exclusion.....	29
2.2	Other reasons for not awarding the Contract.....	30
2.3	Confidentiality and Public Access to Documents.....	30
3.	SELECTION CRITERIA	31
3.1	Professional Information.....	31
3.2	Financial and Economic Capacity	31
3.3	Technical Background	31
4.	AWARD CRITERIA	32
4.1	Quality of the Offer	32
4.2	Price of the Offer	33
5.	AWARD OF THE CONTRACT	33
6.	PAYMENT AND STANDARD CONTRACT	34
7.	VALIDITY	34
8.	LOTS.....	34
9.	ADDITIONAL PROVISIONS.....	34
10.	NO OBLIGATION TO AWARD THE CONTRACT	35
11.	DRAFT CONTRACT	35
12.	SPECIFIC INFORMATION.....	36
12.1	Timetable.....	36
ANNEX I	37
ANNEX II	38
ANNEX III	39
ANNEX IV	41

ANNEX V	42
ANNEX VI.....	43
ANNEX VII.....	44
ANNEX VIII.....	45
ANNEX IX Document CHECKLIST.....	46

PART 1 INTRODUCTION TO ENISA

1. BACKGROUND

Communication networks and information systems have become an essential factor in economic and social development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society. This stems from the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks to the physical infrastructures which deliver services critical to the well-being of European citizens.

For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises, and public sector organisations within the European Union (EU), thus contributing to the smooth functioning of the Internal Market, a European Network and Information Security Agency (ENISA) was established on 10 March 2004¹.

2. SCOPE

The Agency shall assist the European Commission and EU Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the Internal Market, including those set out in present and future Community legislation, such as in the Directive 2002/21/EC.

3. OBJECTIVES

The Agency's objectives are as follows:

- The Agency shall enhance the capability of the Community, EU Member States and, as a consequence, the business community to prevent, to address, and to respond to network and information security problems.
- The Agency shall provide assistance and deliver advice to the Commission and EU Member States on issues related to network and information security falling within its competencies as set out in the Regulation.
- Building on national and Community efforts, the Agency shall develop a high level of expertise.
- The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.
- The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

¹ Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. A "European Community agency" is a body set up by the EU to carry out a very specific technical, scientific or management task within the "Community domain" ("first pillar") of the EU. These agencies are not provided for in the Treaties. Instead, each one is set up by an individual piece of legislation that specifies the task of that particular agency.

4. TASKS

In order to ensure the fulfilment of its objectives, the Agency's tasks will mainly be focused on:

- Advising and assisting the Commission and the Member States on network and information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Collecting and analysing data on security incidents in Europe and emerging risks.
- Promoting risk assessment and risk management methods to enhance our capability to deal with network and information security threats.
- Awareness raising and cooperation between different actors in the network and information security field, notably by developing public-private partnerships in this field.

The Agency shall base its operations on carrying out a work programme adopted in accordance to the relevant Articles of the establishing regulation. The work programme does not prevent the Agency from taking up unforeseen activities that follow its scope and objectives and within the given budget limitations.

5. ORGANISATIONAL FRAMEWORK

The bodies of the Agency comprise a Management Board, an Executive Director (and his staff) and a Permanent Stakeholder Group. The Executive Director is responsible for managing the Agency and performs his/her duties independently.

The Management Board is entrusted with the necessary powers to: establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, approve the Agency's work programme, adopt its own rules of procedure and the Agency's internal rules of operation, appoint and remove the Executive Director. The Management Board should ensure that the Agency carries out its tasks under conditions which enable it to serve in accordance with the Regulation establishing it.

The Permanent Stakeholders Group is composed of experts representing the relevant stakeholders, such as Information and Communication Technologies industry, consumer groups and academic experts in network and information security. The Permanent Stakeholders Group advises the Executive Director in the performance of his duties under the Regulation, in drawing up a proposal for the Agency's work programme and in ensuring communication with the relevant stakeholders on all issues related to the work programme.

The Executive Director will establish, in consultation with the Permanent Stakeholders Group, ad hoc Working Groups composed of experts. Where established, the ad hoc Working Groups shall address in particular technical and scientific matters.

6. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: www.enisa.europa.eu.

For ENISA's legal base please [click here](#).

PART 2 TECHNICAL DESCRIPTION

A. THE PROGRAMME

In its **Communication on Critical Information Infrastructure Protection**² the European Commission highlights the importance of national / governmental CERTs:

*“A strong European early warning and incident response capability has to rely on **well-functioning National/Governmental Computer Emergency Response Teams (CERTs)**, i.e. having a common baseline in terms of capabilities.”* (chapter 3.4.3)

In said Communication ENISA is called upon to support the definition of a **“minimum level of capabilities and services for national / governmental CERTs”** in order to *“establish well functioning national / governmental CERTs in all Member States”* (chapter 5.1)

In the same Communication ENISA is called upon *“to take stock of the results of (pilot) projects and other national initiatives and to [...] **further development and deployment of EISAS.**”* (chapter 5.2)

In the same Communication *“the active role of ENISA is called upon to stimulate and support **pan-European cooperation** between national / governmental CERTs that should lead to enhanced preparedness.”* (chapter 5.3)

In its **Communication “A Digital Agenda for Europe”**³ the European Commission affirms the role of national / governmental CERTs as one key player in the area of trust and security:

*“[...] to react in real-time conditions, a **well functioning and wider network of Computer Emergency Response Teams (CERTs)** should be established in Europe [...]”* (chapter 2.3)

In said Communication the European Commission invites the Member States to act on this: *“Establish by 2012 a well-functioning network of CERTs on national level covering all of Europe”*. (chapter 2.3)

In the same Communication the European Commission highlights that **“Cooperation between CERTs and law enforcement agencies is essential [...]”** (chapter 2.3)

In its Communication *“The EU Internal Strategy in Action: Five steps towards a more secure Europe”*⁴ the European Commission stresses ENISAs role in improving Member States capabilities for dealing with cyber attacks:

² “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” (COM(2009) 149): http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

³ “A Digital Agenda for Europe” (COM(2010) 245): http://ec.europa.eu/information_society/digital-agenda/index_en.htm

⁴ “The EU Internal Strategy in Action: Five steps towards a more secure Europe” (COM(2010) 673): <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/598>

“Overall, ENISA will provide support to these (listed before) actions with the aim of raising standards of CERTs in Europe.” (objective 3, action3)

The three actions are:

- *“Firstly, every Member State [...] should have [...] a **well-functioning CERT**. It is important that [...] **CERTs and law enforcement authorities cooperate**”*
- *“Secondly, Member States should **network together their national / governmental CERTs** [...] to enhance Europe’s preparedness. This activity will also be instrumental in developing [...] a European Information Sharing and Alert System (**EISAS**)”*
- *“Thirdly Member States together with ENISA should [...] undertake regular [...] **exercises in incident response**.”*

Since 2005 **ENISA runs a program dedicated to reinforcing national / governmental CERTs**. The goals of this program are the proliferation of CERTs in Europe in general, support the EU Member States to establish and develop their national / governmental CERTs according to an agreed baseline set of capabilities, to foster and to support the cooperation of CERTs on European and international level and to generally support and reinforce CERT operation and cooperation by making available good practice in (co)operation of national / governmental CERTs.

In particular ENISA;

- together with all relevant stakeholders discusses and develops further a defined set of baseline capabilities for national / governmental CERTs
- supports the Member States in setting-up, training and exercising their national / governmental CERTs, in order to establish a well-functioning network of CERTs on national level
- makes available good practice on various tasks national / governmental CERTs (but also all other CERTs) have to carry out, like incident handling, NIS early warning, etc.
- reinforces cooperation between Member States in general, and the national / governmental CERTs in particular, on European and international level, for example by analysing barriers for cross-border cooperation and proposing measures to tackle them
- supports and facilitates the relationship and cooperation between CERTs and other crucial stakeholders like law enforcement
- develop and deploy further the activities around information sharing and alerting of citizens in the Member States (EISAS)

The results of this tender will contribute to ENISA’s CERT programme.

B. SCOPE OF THIS TENDER

Within the framework of this Open tender procedure, ENISA would like to find suitably qualified contractors to provide the services as stipulated in the technical specifications outlined below. The project has been split into 3 projects defined as LOTS.

A tenderer may bid for one, two, or all three LOTs. The three CERT related projects are outlined below:

LOT No	Subject of the tender	Maximum budget
LOT 1	Operational gaps and overlaps on European level	€ 56,000.00
LOT 2	Proactive detection of network security incidents	€ 45,000.00
LOT 3	Secure communication with the CERTs and other stakeholders	€ 16,000.00

The tenderer is required to provide completely separate technical bids for each LOT. If a tenderer decides to bid for more than one LOT, then the *administrative documentation* required to be provided (as outlined in PART 3 - Section 3: SELECTION CRITERIA and Annexes) can be provided just once.

1 LOT 1: OPERATIONAL GAPS AND OVERLAPS ON EUROPEAN LEVEL

1.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES

In chapter 2.3 of its **Communication “A Digital Agenda for Europe”**⁵ the European Commission states: “[...] to react in real-time conditions, a **well functioning and wider network of Computer Emergency Response Teams (CERTs)** should be established in Europe [...]”.

In its Work Programme for 2011 (WP2011) ENISA included an activity related to supporting CERT (co)operation on European level, which in detail is laid out in Work Package (WPK) 1.4. One of the tasks foreseen in this WPK is an analysis of “Operational gaps and overlaps on European level and how to address them”.

It is crucial to understand, that ENISA does not have an operational role as such, but it may be well suitable to support and facilitate the operations of others by own activities.

With this tender ENISA aims at procuring services in order to carry out an analysis of operational activities that the national / governmental CERTs carry out in order to provide essential services to their constituency. The following activities should be considered as essential:

- Incident Handling (including cooperation with external stakeholders)
- Alerts & Warnings (also referred to as dissemination of NIS relevant information)
- Other services proposed by the prospective contractor

Out of this analysis suggestions should be derived for future activities by ENISA that could:

- complement and facilitate, on European level, activities carried out by national / governmental CERTs (gaps)

⁵ “A Digital Agenda for Europe” (COM(2010) 245): http://ec.europa.eu/information_society/digital-agenda/index_en.htm

- streamline and facilitated, on European level, activities carried out by national / governmental CERTs (overlaps)

The expected result of the work of the prospective contractor is a report (text document) outlining:

- the basic activities that constitute the above mentioned essential services in general
- activities that can be complemented by ENISA (gaps)
- activities where work of ENISA could contribute to avoiding double work (overlaps)

In all suggestions made for future activities, ENISA's mandate and tasks need to be analysed as well and taken into account. ENISA does not have an operational role by mandate, but may be very well suited to support operative tasks in agreement with the Member States and other stakeholders.

It is therefore crucial for ENISA that opinions, positions and ideas of external stakeholders are included in the analysis. It is expected from the tenderer to include in the offer a list of stakeholders, and how they should be involved (see also article 1.9: CONTENT AND PRESENTATION OF THE TECHNICAL OFFER). ENISA can make available to the prospective contractor its own networks and contacts.

The intended target audience for the report will be ENISA CERT experts, and should provide enough insight into the added value ENISA (with its current tasks and mandate) could provide on European level to the smooth functioning of national / governmental CERTs.

1.2 OBJECTIVES AND TASKS

The main objective of this tender is the preparation of a report about operational gaps and overlaps as outlined in article 1.1: "GENERAL DESCRIPTION OF THE REQUIRED SERVICES".

ENISA expects from the tenderer to include in his offer a project plan and a description of the methods proposed to achieve these expected results.

Without anticipating these, it is expected to include at least the following tasks:

1.2.1 TASK 1: Analysis of services

- analysis of the CERT services considered as essential services (namely incident handling and alerts & warnings) in detail, in order to break down services into core activities
- analysis of the CERT services considered as essential services (namely incident handling and alerts & warnings) in a more holistic sense, in order to discover areas and activities that are appropriate to facilitate and support, but are not yet in existence or provided

This task could be realised by desktop research, supplemented by input received from stakeholders (for example in the form of a peer review, or by an initial survey or selected interviews).

1.2.2 TASK 2: Defining areas and activities where gaps or overlaps exist

- analyse the areas and activities derived in Task 1 with regards to gaps that exist, meaning pointing out what would be useful or helpful to have, but what is “not there yet”. Especially of interest is if and how ENISA could tackle these gaps.
- analyse the areas and activities derived in Task 1 with regards to overlaps that exist, meaning pointing out work that is done (for example by each and every national / governmental CERT), which could be also be done by another entity. Especially of interest is if and how ENISA could tackle these overlaps.

This task should be realised in cooperation with selected stakeholders, for example staff members and managers of operating national / governmental CERTs or similar entities.

1.2.3 TASK 3: Deriving concrete suggestions for ENISA

In this phase the areas and activities pointed out in Task 2 should be analysed and aligned with ENISA’s mandate. Wherever necessary the current ENISA mandate must be analysed and interpreted and suitable suggestions for ENISA should be derived. Every suggestion (for an area or an activity to be established or provided by ENISA) should be backed up by the appropriate part of the current ENISA mandate, or its interpretation.

(In addition to this it is possible to point out operational gaps and overlaps which ENISA with its current mandate cannot address!)

This task should be carried out in cooperation with selected stakeholders.

1.2.4 TASK 4: Presentation of the results

The final product is a report; a document that lays out the findings (in the form of suggestions for ENISA), the process that leads to these suggestions and the stakeholders included. The expected document is basically a project report, with the findings / suggestions to ENISA as the main part.

1.3 EXPECTED SKILLS

The performance of the above mentioned activities requires professionals that have good professional multi disciplinary knowledge on all or a sub set of the following fields:

- Very good knowledge of operational aspects of the work of CERTs, especially:
 - Very good know knowledge of the incident handling service and its components
 - Very good knowledge of the alerts & warnings service and its components
 - Very good knowledge of cooperation among CERTs (especially during incident handling)

- Good familiarity of the existing CERT communities (FIRST, TF-CSIRT, etc.)
- Excellent project management skills including quality assurance;
- Very good communication skills.
- Excellent oral and written language skills in English

1.4 DURATION

The duration of this work is foreseen between March 2011 and end of September 2011.

More specifically (*where X = contract signature date*)

- Task 1 should be finalised not later than X + 1 month
- Task 2 should be finalised not later than X + 2 months
- Task 3 should be finalised not later than X + 5 months
- Task 4 should be finalised not later than end of September 2011

1.5 DELIVERABLES

The following deliverables are required from the prospective contractor:

- Monthly progress report on predefined milestones;
- D1 Analysis of essential CERT services (linked to Task 1);
- D2 List of gaps and overlaps (linked to Task 2);
- D3 List of concrete suggestions to ENISA (linked to Task 3)
- D4 Final report (as mentioned in Task 4)

1.6 DURATION OF THE SERVICE

The Tenderer is required to make a proposal in their tender for the time schedule of the activities in order to carry out the project (e.g. including a Gantt chart). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

1.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. The contractor is required to be present at ENISA premises for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) could also be used.

At least the following communication with the contractor is expected.

- One kick off meeting organised either at ENISA premises, or at contractors premises or even at location convenient to both. This meeting needs to take place shortly after the signing of the contract.
- Regular video- or teleconferences on the progress achieved (intervals to be agreed upon)

- On demand provide ENISA with a draft or snapshot of the results produced so far for the deliverables

It should be mentioned that the costs of necessary business trips should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in meetings or other events. Quality assurance, review and final approval of deliverable, and project sign-off will take place at a location to be agreed on later. Informal and regular contacts should be maintained by telephone / Skype / video conferencing and e-mail.

1.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget cannot exceed **56,000.00 Euros (Fifty six thousand Euros)** covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises).

1.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offers to be assessed in terms of quality and of compliance with the Specifications. An Offer shall include a description of the operational means and procedures to be implemented to perform the Contract, supported where appropriate by related documents.

An offer must address each of the following elements as A MINIMUM in order to be considered to be a valid and conforming offer:

- **Description of the skills of the prospective contractor**
 - The Tenderer will have to present its compliance with the expected skills as described in the relevant section.
- **Description of the deliverables**
 - The deliverables must be presented as requested in the section entitled "Deliverables"
 - The requested proposals and additional details (see article 1.5: "DELIVERABLES") must be included in the offer
 - The prospective contractor is expected to provide insights in the methodology chosen in order to produce the deliverables
- **Description of the used methodology / methodologies and additional proposals** (*where appropriate these can be included in the project plan!*)
 - A draft list with stakeholders to be involved during the process (see article 1.2: "OBJECTIVES AND TASKS") should be included in the offer
 - A brief description how those stakeholders will be involved (for example surveys, interviews, workshops, other meetings, etc.) should be included in the offer
 - If appropriate an outline description of additional essential services (see article 1.1: "GENERAL DESCRIPTION OF THE REQUIRED SERVICES") should be included in the offer

- **Management of provision of services**
 - Project Management: a close description of the project management method used including quality assurance is required. Breakdown of tasks, definition of milestones, assignment of person days to tasks, etc. should be presented in a concise project plan (including a Gantt chart) and included in the offer.
 - At the kick off meeting, the project plan will be confirmed as final.
 - The prospective contractor must also identify possible risks to the project and propose mitigation measures.

- **In addition the prospective contractor is expected to highlight / explain**
 - Availability and ability of the Contractor to respond: prompt availability of resources is required within the specified delivery timeframes. Additionally, any ancillary or support resources, such as a network of associates to support the scope of this Call for Tenders must be clearly stated.

- Short CV's of the experts that will be allocated in the project focussing on their experience and expertise on the areas covered by the study.

2. LOT 2 - PROACTIVE DETECTION OF NETWORK SECURITY INCIDENTS

2.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES

In its **Communication “A Digital Agenda for Europe”** the European Commission affirms the role of national / governmental CERTs as one key player in the area of trust and security:

“[...] to react in real-time conditions, a well functioning and wider network of Computer Emergency Response Teams (CERTs) should be established in Europe [...]”. (chapter 2.3)

In its Work Programme for 2011 (WP2011) ENISA included the activity related to examination of the area of good practice for early warning for CERTs, which in detail is laid out in Work Package (WPK) 2.4. One of the tasks foreseen in this WPK is an analysis of “Early Warning for NIS – Status Quo and further development”.

With this tender ENISA aims at procuring services in order to:

- do the stocktaking of available methods, activities and information sources (hereafter *measures*) for proactive detection of network security incidents, which are used already or potentially could be used by national / governmental and other CERTs
- analyse the benefits and shortcomings of the identified measures
- identify good practice and recommended measures for new and already established national / governmental and other CERTs
- outline possible further activities in order to mitigate the common shortcomings identified during the analysis, including tasks and roles of different stakeholders.

It is crucial for ENISA that opinions, positions and ideas of external stakeholders are included in the analysis. It is expected from the tenderer to include in the offer groups of stakeholders, and how they should be involved (e.g. participation in a survey, expert group etc) (see also article 2.9: “Content and presentation of the technical offer”). ENISA can make available to the prospective contractor its own networks and contacts.

The expected result of the work of the prospective contractor is a report (text document) laying out the details and results of the tasks described above (please see also article “Objectives and tasks” for more details).

The intended target audience for this report will be the managers and technical staff of national / governmental CERTs. However the report can be useful for any other CERT or abuse team as well.

2.2 OBJECTIVES AND TASKS

The prospective contractor will need to develop the comprehensive report on the existing measures which are used already or can be recommended for use by national / governmental and other CERTs for proactive detection of network security incidents, as opposed to passive waiting for incoming incident reports. Also possible further activities in order to mitigate the common shortcomings of the measures identified, including tasks and roles of different stakeholders, need to be analysed.

The final report would serve as a reference point for both newly established CERTs to identify the appropriate measures to do proactive detection of incidents, and already established CERTs as a means to get more ideas on how to improve the set of measures they use.

ENISA expects from the tenderer to include in his offer a project plan and a description of the methods proposed to achieve these expected results.

Without anticipating these, it is expected to include at least the following tasks or offer an alternative approach how to achieve the same or better result:

2.2.1 TASK 1: Desktop research of the existing measures

- gather information on the methods, activities and information sources (internal, external, public, closed, commercial etc) already used or which can be used by CERTs to proactively detect incidents in the networks of their constituency, as opposed to the passive handling of incoming incident reports
- using the existing related knowledge and experience in the prospective contractor's team (needs to be described in the offer)
- using the information available on the internet and in other sources about the measures that can be used by CERTs to proactively detect incidents

2.2.2 TASK 2: Survey of CERTs in Europe

- run the survey among known CERTs in Europe to gather input on actual measures currently used or planned to be implemented
- ENISA can provide contacts

2.2.3 TASK 3: Establishing expert group, initiating, moderating discussions

- some examples of the possible tasks of the group:
 - gather additional input on measures
 - discuss open questions during the other tasks
 - validate the results of the analysis (see Task 4)
- describe in the offer (see article 2.9: "Content and presentation of the technical offer") what groups of stakeholders need to be involved, in what stages of the project the expert group would be involved, how the work of the group would be arranged, e.g., online or physical meetings, e-mail mailing list etc
- ENISA can make available to the prospective contractor its own contacts.

2.2.4 TASK 4: Analysis of the measures identified

- analyse the benefits and shortcomings of the measures identified during the desktop research, survey, expert group discussions
- in the offer tenderer needs to outline a proposed set of criteria for evaluation, e.g., complexity of implementation, accuracy of the results provided, etc (see article 2.9: "Content and presentation of the technical offer")
- identify good practice and recommended measures for new and already established national / governmental and other CERTs
- identify common shortcomings of the available measures and analyse the ways for their mitigation, including possible tasks and roles of different stakeholders

2.2.5 TASK 5: Presentation of the results

The final product is a report. Its structure needs to be outlined in the offer (see article 2.9: "Content and presentation of the technical offer").

The layout of the final report should be chosen as to make possible updates of the content in the future easier.

The report should contain:

- the description of the work carried out
- the inventory of the measures identified, their description, evaluation
- the set of measures recommended for use by national / governmental and other CERTs
- recommendations on how to address common shortcomings of the identified measures, including possible tasks and roles of different stakeholders.

2.3 EXPECTED SKILLS

The performance of the above mentioned activities requires professionals that have good professional multi disciplinary knowledge on all or a sub set of the following fields:

- Very good understanding of the operation of computer networks (Internet, WAN, LAN) including core protocols, protocol stacks etc
- Very good understanding of general information and network security principles, including security incident handling
- Experience in developing, deploying and/or using internet "early warning systems", including network monitoring, proactive incident detection measures in production environments
- Experience in security incident handling, including communication with different external stakeholders (e.g., while working for CERT or abuse team)
- Experience in performing surveys, leading thematic expert groups and writing reports
- Excellent project management skills including quality assurance and risk management
- Very good communication skills
- Excellent oral and written language skills in English

2.4 DURATION

The duration of this work is foreseen between March 2011 and end of September 2011.

More specifically (*where X = contract signature date*)

- Task 1 and 2 should be finalised not later than X + 2 months
- Task 3 and 4 should be finalised not later than X + 4 months
- Task 5 should be finalised not later than end of September 2011 with the complete final draft report available for the review by ENISA by September 16, 2011

2.5 DELIVERABLES

The following deliverables are required from the prospective contractor:

- Monthly progress report on predefined milestones;
- D1 If part of the approved project plan, an interim internal report with the analysis of the results of the CERT survey and the desktop research
- D2 If part of the approved project plan, provide necessary resources (eg, means of communication, meetings etc) for successful work of the expert group during the project according to the approach described in the offer (see article 2.9: “Content and presentation of the technical offer”)
- D3 Final draft report
- D4 Final report

2.6 DURATION OF THE SERVICE

The Tenderer is required to make a proposal in their tender for the time schedule of the activities in order to carry out the project (e.g. including a Gantt chart). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

2.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the contractor’s premises. The contractor is required to be present at ENISA premises for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) could also be used.

At least the following communication with the contractor is expected.

- One kick off meeting (physical or online)
- Teleconferences related to the project milestones in the agreed project plan
- Regular teleconferences on the progress achieved (intervals to be agreed upon)

It should be mentioned that the costs of possible business trips, expert group meetings and communication should be included in the total offer. ENISA will not additionally reimburse the contractor the related costs.

Quality assurance, review and final approval of deliverable, and project sign-off will take place at a location to be agreed on later. Informal and regular contacts should be maintained by telephone and e-mail.

2.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget cannot exceed **45,000.00 Euros (forty five thousand Euros)** covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA’s premises, provision of expert group communications and meetings).

2.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offers to be assessed in terms of quality and of compliance with the Specifications. An Offer shall include a description of the operational means and procedures to be implemented to perform the Contract, supported where appropriate by related documents.

An offer must address each of the following elements as A MINIMUM in order to be considered to be a valid and conforming offer:

- **Description of the skills of the prospective contactor**
 - The Tenderer will have to present its compliance with the expected skills as described in the relevant article.
- **Description of the deliverables**
 - The proposed structure of the final report needs to be part of the offer
 - The deliverables must be presented as requested in the article entitled “Deliverables”
- **The prospective contractor is expected to provide insights in the methodology (approach) chosen in order to reach the objectives of the project described above in article “Objectives and tasks”. In particular:**
 - A proposed set of criteria for the evaluation of different identified measures for proactive detection of incidents (e.g., complexity of implementation, accuracy of the results provided, etc)
 - Proposed stakeholders / stakeholder groups and how they will be involved (e.g., participation in a survey, expert group etc)
 - If the expert group will be part of the approach chosen, details need to be provided on what stakeholder groups would be involved, how the work of the expert group would be organised (e.g., physical meetings, e-mail mailing lists, video conferences etc), in what stages of the project the expert group would be involved
- **Management of provision of services**
 - Project Management: a close description of the project management method used including quality assurance is required. Breakdown of tasks; milestones definition; assignment of experts to tasks and person days to tasks should be presented in a Gantt chart, included in the offer
 - At the kick off meeting, the project plans will be confirmed as final
 - The prospected contactor must also identify possible risks to the project and propose mitigation measures
- **In addition the prospective contractor is expected to highlight / explain**
 - Availability and ability of the tenderer to respond: prompt availability of resources is required within the specified delivery timeframes. Additionally, any ancillary or support resources, such as a network of associates to support the scope of this Call for Tenders must be clearly stated
- Short CV’s of the experts that will be allocated in the project focussing on their experience and expertise on the areas covered by the study.

3. LOT 3 - SECURE COMMUNICATION WITH THE CERTs & OTHER STAKEHOLDERS

3.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES

In its Work Programme for 2011 (WP2011) ENISA included an activity related to reinforcing CERTs in the Member States, which in detail is laid out in Work Package (WPK) 1.3.

One of the tasks foreseen in this WPK is an analysis of “ways to improve communication with the CERTs and other stakeholders (institutions in the Member States, European Commission, etc.), especially when it comes to sharing information in a secure way. ‘Secure’ in this respect means transportation of information, assuring confidentiality, integrity and authenticity of the data”.

With this tender ENISA aims at procuring services in order to create a proposal for a channel(s) for secure communication with the CERTs and other varying stakeholders and a roadmap for implementation of such a channel(s) and future development.

The channel should be suited for frequently changing participants. ENISA CERT experts are the intended target audience for this report and roadmap. The final product should be a report.

3.2 OBJECTIVES AND TASKS

The main objective of this tender is the preparation of a report for secure communication channel(s) with the CERTs and other stakeholders and a roadmap for implementation of such a channel(s) and future development as outlined in article 3.1: “General description of the required services”.

ENISA expects from the tenderer to include in his offer a project plan and a description of the methods proposed to achieve these expected results.

Without anticipating this proposal, it is expected to include at least the following tasks:

3.2.1 TASK 1: Stock taking of existing solutions

A stock taking should be held in order to have an overview of existing solutions for secure information channels. It should also cover current developments and research in that area. Special attention should go to the pros and cons of the different solutions.

These studies can include desktop research, discussions with experts, internal knowledge and expertise, and/or other possible means. A market survey could be part of this stock taking.

3.2.2 TASK 2: Analysis of the requirements

The requirements of the different stakeholders (CERTs, institutions in the Member States, European Commission, etc.) should be analysed in order to reveal the needs with regard to improving the security of the communication between these stakeholders.

3.2.3 TASK 3: Provide a practical guide/roadmap for a suitable channel to start with

Based on the stock taking of existing solutions and the analysis of the requirements of the different stakeholders, the tenderer should provide a practical guide and a proposal for a roadmap for implementing such a secure channel. It is clear that this practical guide and roadmap must use the input given by the stakeholders.

3.2.4 TASK 4: Project management

The objective of this task is to define and implement the necessary management mechanisms, sound planning and resource allocation in order to manage this project.

As part of this task the contractor should interact with ENISA staff and external experts, and provide ENISA with regular management reporting. This way the punctual delivery of good quality results of this project, within the budget allocated, will be ensured.

3.2.5 TASK 5: Presentation of the results

The key objective of this tender is the compilation of a report. It should include the results of the stock taking as mentioned in Task 1, the analysis of the requirements of the various stakeholders as mentioned in Task 2 and provide a practical guide/roadmap for a suitable channel to start with as described in Task 3.

3.3 EXPECTED SKILLS

The performance of the above mentioned activities requires professionals that have good professional multi disciplinary knowledge on all or a sub set of the following fields:

- Excellent project management skills including quality assurance;
- Very good communication skills
- Excellent oral and written language skills in English
- Proven experience in organising stock taking exercises, analysis skills, and creating good reports and recommendations on relevant subjects
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements
- Good professional experience in relevant information security issues and disciplines (e.g. security policies and controls)
- Good familiarity with applied cryptography
- Good understanding of security issues involved in communication
- Proven professional and/or academic experience in communication security

3.4 DURATION

The duration of this work is foreseen between March 2011 and end of September 2011.

Please provide a proposal for appropriate milestones (based on the deliverables shown in Article 3.5 below) in your project plan.

3.5 DELIVERABLES

The following deliverables are required from the Contractor:

- Monthly progress report on predefined milestones;
- D1 Stock taking of existing solutions and their characteristics
- D2 Analysis report of the requirements of the stakeholders
- D3 Practical guide/roadmap for a suitable channel to start with

3.6 DURATION OF THE SERVICE

The Tenderer is required to make a proposal in their tender for the time schedule of the activities in order to carry out the project (e.g. including a Gantt chart). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this procurement.

3.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. The contractor is required to be present at ENISA premises for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) could also be used.

As a minimum, it is expected to have regular teleconferences on the progress achieved (intervals to be agreed upon).

It should be mentioned that the costs of business trips (if applicable) should be included in the total offer.

Quality assurance, review and final approval of deliverable, and project sign-off will take place at a location to be agreed on later. Informal and regular contacts should be maintained by telephone and e-mail.

3.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget cannot exceed **16,000.00 Euros (Sixteen thousand Euros)** covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises if applicable).

3.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offers to be assessed in terms of quality and of compliance with the Specifications. An Offer shall include a description of the operational means and procedures to be implemented to perform the Contract, supported where appropriate by related documents.

An offer must address each of the following elements as A MINIMUM in order to be considered to be a valid and conforming offer:

- **Description of the skills of the expected contactor**
 - The Tenderer will have to present its compliance with the expected skills as described in the relevant section.
- **Description of the deliverables**
 - The deliverables must be presented as requested in section entitled “Deliverables”
 - The requested proposals and additional details (see section “Deliverables”) must be included in the offer
 - The prospective contractor is expected to provide insights in the methodology chosen in order to produce the deliverables
- **The prospective contractor is expected to provide their proposals on the following:**
 - A structure for the final report
 - Some methodologies for the stock taking, i.e. a market survey.
 - Characteristics of security solutions enabling to compare and clearly see the pros and cons of the different solutions. This should be a in the form of a structure or a list.
- **Management of provision of services**
 - Project Management: a close description of the project management method used including quality assurance is required. Breakdown of tasks; milestones definition; assignment of experts to tasks and person days to tasks should be presented in a Gantt chart, included in the offer.
 - At the kick off of this project, the project plans will be confirmed as final. This can happen during a teleconference or a video conference.
 - The prospective contractor must also identify possible risks to the project and propose mitigation measures.
- **In addition the prospective contractor is expected to highlight / explain**
 - Availability and ability of the Contractor to respond: prompt availability of resources is required within the specified delivery timeframes. Additionally, any ancillary or support resources, such as a network of associates to support the scope of this Call for Tenders must be clearly stated.
- Short CV's of the experts that will be allocated in the project focussing on their experience and expertise on the areas covered by the study.

The following specifications are common to BOTH LOTS:

4. CONTENT AND PRESENTATION OF THE PRICE OFFER

The Price offer(s) must be drawn up using the Financial Offer template provided (see Annex IV).

5. PRICE

Prices submitted in response to this Tender must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in Euro and VAT excluded.

6. PRICE REVISION

Prices submitted in response to this Tender shall be fixed and not subject to revision.

7. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER

ENISA will not reimburse any costs incurred in the preparation and submission of a Tender. Any such costs must be paid by the Tenderer.

8. PERIOD OF VALIDITY OF THE TENDER

Tenderers must enclose a confirmation that the prices given are valid for (90) ninety days from the date of submission of the tender.

9. PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Tenderers must therefore give prices which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

10. PAYMENT ARRANGEMENTS

Payments under the Contract shall be carried out subject to prior approval of the Services by ENISA within 30 days after an invoice is submitted to ENISA. One single payment will be made after receipt and approval of the deliverables by ENISA. An invoice must specify the specific deliverables covered. A note that accompanies the final deliverables must present the resources used for each of the deliverables presented. Time sheets should be submitted as appropriate.

11. CONTRACTUAL DETAILS

A model of the Service Contract is proposed to the successful candidate(s) - see Annex V.

Please note that the general conditions of our standard service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. It is strongly recommended that you have this draft contract checked and passed by your legal section before committing to submitting an offer.

PART 3 ADMINISTRATIVE DETAILS

1. FORMAL REQUIREMENTS

1.1 Address and deadline for submission of the Tender:

You are invited to tender for this project and requested to submit your tender no later than **01 February 2010** either by:

- a) **Registered post or express courier**. The postal service's dated stamp or the courier company's printed delivery slip and stamp will constitute proof of compliance with the deadline given above:

or

- b) **Hand-delivery** (direct or through any authorised representative of the Tenderer) by 17.00 hours on **01 February 2010** at the latest to the address shown below (please, be informed that only delivery during working hours 09:00-17:00 hrs, is accepted). In the case of hand-delivery, in order to establish proof of the date of deposit, the depositor will receive from an official at the below-mentioned address, a receipt which will be signed by both parties, dated and time stamped.

Please note that in this case it is the date and time actually received at the ENISA premises that will count.

Please Note: Due to frequent delays encountered with the postal services in Europe, we would ***strongly suggest that you use a courier service***. It is important to avoid delays to the programmed Opening and Evaluation dates as this will in turn delay the contract award, thereby affecting project completion dates.

The offer must be sent to one of the following addresses:

Postal Address		Express Courier & Hand Delivery
European Network and Information Security Agency (ENISA) For the attention of: The Procurement Officer PO Box 1309 71001 Heraklion Greece	or	European Network and Information Security Agency (ENISA) For the attention of Procurement Section Science and Technology Park of Crete (ITE) Vassilika Vouton 700 13 Heraklion Greece

Please note that late delivery will lead to exclusion from the award procedure for this Contract.

1.2 Presentation of the Offer and Packaging

The offer (consisting of one original and two copies) should be enclosed in two envelopes, both of which should be sealed. If self-adhesive envelopes are used, they should be further sealed with adhesive tape, upon which the Tenderer's signature must appear.

The **outer envelope**, in addition to the above-mentioned ENISA address, should be marked as follows:

OPEN CALL FOR TENDER NO. ENISA P/35/10/TCD
“Reinforcing operational aspects of national / governmental CERTs”
NOT TO BE OPENED BY THE MESSENGER/COURIER SERVICE
NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE 10th FEB 2011
TENDERED BY THE FIRM: <PLEASE INSERT NAME OF THE TENDERER/COMPANY>

The **inner envelope** should also be similarly marked:

OPEN CALL FOR TENDER NO. ENISA P/35/10/TCD
“Reinforcing operational aspects of national / governmental CERTs”
NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE 10th FEB 2011
TENDERED BY THE FIRM: <PLEASE INSERT NAME OF THE TENDERER/COMPANY>

1.3 Identification of the Tenderer

Tenderers are required to complete the **Legal Entity Form (Annex I)** which must be signed by a representative of the Tenderer authorised to sign contracts with third parties. There is one form for 'individuals', one for 'private entities' and one for 'public entities'. A standard form is provided for each category - please choose whichever is applicable. In addition to the above, a **Financial Identification Form** must be filled in and signed by an authorised representative of the Tenderer and his/her bank (or a copy of the bank account statement instead of bank's signature). A specimen form is provided in **Annex II**. Finally a **Declaration by Authorised Representative (Annex VI)** must also be completed for internal administrative purposes.

The **Legal Entity Form** must be supported by the following documents relating to each Tenderer in order to show its name, address and official registration number:

a) For private entities:

- A legible copy of the instrument of incorporation or constitution, and a copy of the statutes, if they are contained in a separate instrument, or a copy of the notices of such constitution or incorporation published in the national or other official journal, if the legislation which applies to the Tenderer requires such publication.
- If the instruments mentioned in the above paragraph have been amended, a legible copy of the most recent amendment to the instruments mentioned in the previous indent, including that involving any transfer of the registered office of the legal entity, or a copy of the notice published in the relevant national or other official journal of such amendment, if the legislation which applies to the Tenderer requires such publication.
- If the instruments mentioned in the first paragraph have not been amended since incorporation and the Tenderer's registered office has not been transferred since then, a written confirmation, signed by an authorised representative of the Tenderer, that there has been no such amendment or transfer.
- A legible copy 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.
- If the above documents do not show the registration number, a proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or any other official document showing the registration number.
- If the above documents do not show the VAT number, a copy of the VAT registration document, where applicable.

b) For Individuals:

- A legible copy of their identity card or passport.
- Where applicable, a proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or any other official document showing the registration number.
- If the above documents do not show the VAT number, a copy of the VAT registration document, where applicable.

c) For Public Entities:

- A copy of the resolution decree, law, or decision establishing the entity in question or failing that, any other official document attesting to the establishment of the entity.

All tenderers must provide their Legal Entity Form (Annex I) as well as the evidence mentioned above.

In case of a joint bid, only the co-ordinator must return the Financial Identification form (Annex II).

The Tenderer must be clearly identified, and where the Tender is submitted by an organisation or a company, the following administrative information and documents must be provided:

Full name of organisation/company, copy of legal status, registration number, address, person to contact, person authorised to sign on behalf of the organisation (copy of the official mandate must be produced), telephone number, facsimile number, VAT number, banking details: bank name, account name and number, branch address, sort code, IBAN and SWIFT address of bank: a bank identification form must be filled in and signed by an authorised representative of each Tenderer and his banker.

Tenders must be submitted individually. If two or more applicants submit a joint bid, one must be designated as the lead Contractor and agent responsible.

1.4 Participation of consortia

Consortia, may submit a tender on condition that it complies with the rules of competition. The 'Consortium Form' (Annex VII) must be completed and submitted with your offer.

A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific tender procedure. Such a grouping (or consortia) must specify the company or person heading the project (the leader) and must also submit a copy of the document authorising this company or person to submit a tender. All members of a consortium (i.e., the leader and all other members) are jointly and severally liable to the Contracting Authority.

In addition, each member of the consortium must provide the required evidence for the exclusion and selection criteria (*Articles 2 and 3 below*). Concerning the selection criteria "technical and professional capacity", the evidence provided by each member of the consortium will be checked to ensure that the consortium as a whole fulfils the criteria.

The participation of an ineligible person will result in the automatic exclusion of that person. In particular, if that ineligible person belongs to a consortium, the whole consortium will be excluded.

1.5 Subcontracting

In well justified cases and subject to approval by ENISA, a contractor may subcontract parts of the services. The 'Sub-contractors Form' (Annex VIII) must be completed and submitted with your offer.

Contractors must state in their offers what parts of the work, if any, they intend to subcontract, and to what extent (% of the total contract value), specifying the names, addresses and legal status of the subcontractors.

The sub-contractor must not sub-contract further.

Sub-contractors must satisfy the eligibility criteria applicable to the award of the contract. If the identity of the intended sub-contractor(s) is already known at the time of submitting the tender, all sub-contractors must provide the required evidence for the exclusion and selection criteria.

If the identity of the sub-contractor is not known at the time of submitting the tender, the tenderer who is awarded the contract will have to seek ENISA's prior written authorisation before entering into a sub-contract.

Where no sub-contractor is given, the work will be assumed to be carried out directly by the bidder.

1.4 Signatures of the Tender

Both the technical and the financial offer must be signed by the Tenderer's authorised representative or representatives (preferably in blue ink).

1.5 Total fixed price

A total fixed price expressed in Euro must be included for each LOT in the Tender. The contract prices shall be firm and not subject to revision.

1.6 Language

Offers shall be submitted in one of the official languages of the European Union (preferably in English).

1.7 Opening of the Tenders

The public opening of received tenders will take place on **10th February 2011 at 10:00am** at ENISA Building, Science and Technology Park of Crete, GR - 70013 Heraklion, Greece.

A maximum one legal representative per participating tenderer may attend the opening session. Tenderers shall inform the Agency in writing of their intention to attend, at least 48 hours prior to the opening session.

2. GROUNDS FOR EXCLUSION OF TENDERERS

2.1 Reasons for Exclusion

Pursuant to Article 29 of Council Directive 92/50/EC relating to Public Service Contracts and to Article 93 of the Financial Regulation, ENISA will exclude Tenderers from participation in the procurement procedure if:

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;

They have been convicted of an offence concerning their professional conduct by a judgement which has the force of res judicata;

They have been guilty of grave professional misconduct proven by any means which the contracting authority can justify;

They have not fulfilled obligations relating to the payment of social security contributions or 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;

- They have been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;
- Following another procurement procedure or grant award procedure financed by the Community budget, they have been declared to be in serious breach of contract for failure to comply with their contractual obligations.

Tenderers must certify that they are not in one of the situations listed in sub-article 2.1 (see Annex III: Exclusion criteria and non-conflict of interest form). If the tender is proposed by a consortium this form must be submitted by each partner.

2.2 Other reasons for not awarding the Contract

Contracts may not be awarded to Candidates or Tenderers who, during the procurement procedure:

- a. Are subject to a conflict of interest;
- b. Are guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the contract procedure or fail to supply this information;
- c. Any attempt by a Tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or ENISA during the process of examining, clarifying, evaluating and comparing tenders will lead to the rejection of his offer and may result in administrative penalties.

See last paragraph point 2.1.

2.3 Confidentiality and Public Access to Documents

In the general implementation of its activities and for the processing of tendering procedures in particular, ENISA observes the following EU regulations:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;

- Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

3. SELECTION CRITERIA

The following criteria will be used to select the Tenderers. If the Tender is proposed by a consortium these criteria must be fulfilled by each partner.

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.1 Professional Information

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers, in country of establishment.

3.2 Financial and Economic Capacity

Proof of financial and economic standing may be furnished by one or more of the following references:

- Annual accounts, balance sheet or extracts there from where publication of the balance sheet is required under company law in the country of establishment;
- Statement of the undertaking's overall turnover and its turnover in respect of the services to which the contract relates for the previous two financial years.

If, for any valid reason, the service provider is unable to provide the references requested by the contracting authority, he may prove his economic and financial standing by any other document which the contracting authority considers appropriate.

3.3 Technical Background

3.3(a) For LOT 1 - Operational gaps and overlaps on European level:

A curriculum vitae of the Tenderer, as well as of all members of the Tenderer's team, has to be included, in which the Tenderer has to make statements about (in line with Part 2 – Art 1.3 for LOT 1 - Required Skills):

- His technical knowledge and experience in the relevant technical areas (including references to projects similar to the one proposed by this tender);
- His management capability (including, but not limited to, project management in a European context and quality assurance).

3.3(b) For LOT 2 - Proactive detection of network security incidents:

A curriculum vitae of the Tenderer, as well as of all members of the Tenderer's team, has to be included, in which the Tenderer has to make statements about (in line with Part 2 – Art 2.3 for LOT 2 - Required Skills):

- His technical knowledge and experience in the relevant technical areas;
- His management capability (including, but not limited to, project management and quality assurance).

3.3(c) For LOT 3 - Secure communication with the CERTs and other stakeholders:

A curriculum vitae of the Tenderer, as well as of all members of the Tenderer's team, has to be included, in which the Tenderer has to make statements about (in line with Part 2 – Art 3.3 for LOT 3 - Required Skills):

- His technical knowledge and experience in the relevant technical areas (including references to projects similar to the one proposed by this tender), and more specifically in the field of applied cryptography;
- His management capability (including, but not limited to, project management in a European context and quality assurance).

4. AWARD CRITERIA

The following award criteria apply to LOTS 1, 2 and 3 identically:

4.1 Quality of the Offer

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed on the basis of the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	Technical compliance	Compliance with the technical descriptions (part 2 of this document)	30/100
2.	Quality and accuracy of content and structure	Quality of the proposal and accuracy of the description to provide the requested services	25/100
3.	Project Team	Composition of project team, direct involvement of senior staff, and distributions of tasks amongst experts; proposed workflows and quality review cycles	30/100
4.	Methodology	Selected methodology and project management	10/100
Total Qualitative Points (QP)			100

Minimum attainment per criterion

Offers scoring less than 50% for any criterion will be deemed to be of insufficient quality and eliminated from further consideration.

Minimum attainment overall

Offers scoring less than 60% after the evaluation process will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all criteria gives a total of 100 points. The respective weighting between the different awards criteria depends on the nature of the services required and is consequently closely related to the terms of reference. The award criteria are thus quantified parameters that the offer should comply with. The **qualitative award criteria** points will be weighted at **70%** in relation to the price.

4.2 Price of the Offer

Tenders must state a total fixed price in Euro. Prices quoted should be exclusive of all charges, taxes, dues including value added tax in accordance with Article 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Such charges may not therefore be included in the calculation of the price quoted.

ENISA, in conformity with the Protocol on the Privileges and Immunities of the European Community annexed to the Treaty of April 8th, 1965, is exempt from all VAT.

Offers exceeding the maximum price set in Part 2; Article 1.8 for LOT 1; Article 2.8 for LOT 2 and Article 3.8 for LOT 3 will be excluded. The cheapest offer will receive the maximum points and the rest of the candidate's offers will be awarded points in relation to the best offer as follows

$$PP = (PC / PB) \times 100$$

Where;

- PP** = Weighted price points
- PC** = Cheapest bid price received
- PB** = Bid price being evaluated

5. AWARD OF THE CONTRACT

The contract for each Lot will be awarded to the offer which is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation

on the basis of the ratio between the **quality criteria (70%)** and the **price (30%)**. The following formula will be used:

$$\text{TWP} = (\text{QP} \times 0.7) + (\text{PP} \times 0.3)$$

where;

QP = Qualitative points

PP = Weighted price points

TWP = Total weighted points score

6. PAYMENT AND STANDARD CONTRACT

Payments under the Service Contract shall be made in accordance with article I.5 of the Special Conditions and article II.4.3 of the General Conditions (see Annex V)

In drawing up their bid, the Tenderer should take into account the provisions of the standard contract which include the “General terms and conditions applicable to contracts”

7. VALIDITY

Period of validity of the Tender: 90 days from the closing date given above. The successful Tenderer must maintain its Offer for a further 220 days from the notification of the award.

8. LOTS

This Tender is divided into three Lots.

- **LOT 1:** Operational gaps and overlaps on European level
- **LOT 2:** Proactive detection of network security incidents
- **LOT 3:** Secure communication with the CERTs and other stakeholders

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 ENISA and will be regarded as confidential.

10. NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on ENISA to award the contract. Should the invitation to tender cover several items or lots, ENISA reserves the right to award a contract for only some of them. ENISA 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.

11. DRAFT CONTRACT

A Service Contract will be proposed to the selected candidate for each LOT. A draft copy of which is included as Annex V to this tender.

Please note that the general conditions of our standard service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. It is strongly recommended that you have this draft contract checked and passed by your legal section before committing to submitting an offer.

12. SPECIFIC INFORMATION

12.1 Timetable

The timetable for this tender and the resulting contract(s) is as follows:

Title: **“Reinforcing operational aspects of national / governmental CERTs”**

ENISA P/35/10/TCD

Summary timetable comments

Launch of tender - Contract notice to the Official Journal of the European Union (OJEU)	15 December 2010	
Deadline for request of information from ENISA	26 January 2011	
Last date on which clarifications are issued by ENISA	28 January 2011	
Deadline for submission of offers	01 February 2011	in case of hand-delivery (05:00 pm local time. This deadline is fixed for the receipt of the tender in ENISA's premises)
Opening of offers	10 February 2011	At 10:00 Greek time
Date for evaluation of offers	10 February 2011	At 11:00 Greek time
Notification of award to the selected candidate	3 rd week of February 2011	Estimated
14 day standstill period	mid March 2011	Estimated
Contract signature	mid March 2011	Estimated
Commencement date of activities	As per tender	Estimated
Completion date of activities	As per tender	Estimated

ANNEX I

Legal Entity Form

The specific form, for either a;

- c) public entity,
- d) private entity or
- e) individual entity,

is available for download in each of the 22 official languages at the following address: http://ec.europa.eu/budget/execution/legal_entities_en.htm

Please download the appropriate form, complete the details requested and include in your tender offer documentation.

ANNEX II

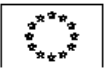
FINANCIAL IDENTIFICATION FORM

- SPECIMEN FOR THE TENDERER -

(to be completed by the Tenderer and his financial institution)

The Tenderer's attention is drawn to the fact that this document is a sample only, and a specific form in each of the 22 official languages is available for download at the following address:

http://ec.europa.eu/budget/execution/ftiers_en.htm

	FINANCIAL IDENTIFICATION
PRIVACY STATEMENT	http://ec.europa.eu/budget/execution/ftiers_fr.htm
ACCOUNT NAME	
ACCOUNT NAME ⁽¹⁾	<input type="text"/>
	<input type="text"/>
ADDRESS	<input type="text"/>
	<input type="text"/>
TOWN/CITY	<input type="text"/>
POSTCODE	<input type="text"/>
COUNTRY	<input type="text"/>
CONTACT	
CONTACT	<input type="text"/>
TELEPHONE	<input type="text"/>
FAX	<input type="text"/>
E - MAIL	<input type="text"/>
BANK	
BANK NAME	<input type="text"/>
	<input type="text"/>
BRANCH ADDRESS	<input type="text"/>
	<input type="text"/>
TOWN/CITY	<input type="text"/>
POSTCODE	<input type="text"/>
COUNTRY	<input type="text"/>
ACCOUNT NUMBER	<input type="text"/>
IBAN ⁽²⁾	<input type="text"/>
REMARKS:	<input type="text"/>
BANK STAMP + SIGNATURE OF BANK REPRESENTATIVE (Both Obligatory) ⁽³⁾	DATE + SIGNATURE ACCOUNT HOLDER : (Obligatory)
<input type="text"/>	DATE <input type="text"/>
<small>⁽¹⁾ The name or title under which the account has been opened and not the name of the authorized agent ⁽²⁾ If the IBAN Code (International Bank account number) is applied in the country where your bank is situated ⁽³⁾ It is preferable to attach a copy of recent bank statement, in which event the stamp of the bank and the signature of the bank's representative are not required. The signature of the account-holder is obligatory in all cases.</small>	

ANNEX III

DECLARATION OF HONOUR

WITH RESPECT TO THE

EXCLUSION CRITERIA AND ABSENCE OF CONFLICT OF INTEREST

The undersigned: *(Please print name)*

in his/her own name *(if the economic operator is a natural person)*

or

representing *(if the economic operator is a legal entity)*

Official name of the company/organisation:

.....

Official legal form:

Official address in full:

.....

.....

VAT (Tax) registration number:

.....

Declares that the company or organisation that he/she represents:

- is not bankrupt or being wound up, is not having its affairs administered by the courts, has not entered into an arrangement with creditors, has not suspended business activities, is not the subject of proceedings concerning those matters, and is not in any analogous situation arising from a similar procedure provided for in national legislation or regulations;
- has not been convicted of an offence concerning professional conduct by a judgment which has the force of *res judicata*;
- has not been guilty of grave professional misconduct proven by any means which the contracting authorities can justify;
- has fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which it is established or with those of the country of the contracting authority or those of the country where the contract is to be performed;

- has not been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;
- has not been declared to be in serious breach of contract for failure to comply with his contractual obligations subsequent to another procurement procedure or grant award procedure financed by the Community budget.

In addition, the undersigned declares on his honour:

- that on the date of submission of the tender, the company or organisation he represents and the staff proposed for this tender are not subject to a conflict of interests in the context of this invitation to tender; he undertakes to inform the ENISA Agency without delay of any change in this situation which might occur after the date of submission of the tender;
- that the information provided to the ENISA Agency within the context of this invitation to tender is accurate, truthful and complete.

By signing this form, the undersigned acknowledges that they have been acquainted with the administrative and financial penalties described under art 133 and 134 b of the Implementing Rules (Commission Regulation 2342/2002 of 23/12/02), which may be applied if any of the declarations or information provided prove to be false

.....
Full name

.....
Signature

.....
Date

ANNEX IV

FINANCIAL OFFER:

“Reinforcing operational aspects of national / governmental CERTs”

ENISA P/35/10/TCD

Please provide your financial lump sum offer for **LOT 1 and/or LOT 2 and/or LOT 3**

LOT Description:	Number of 'Person days' required for completion of project.	Your OFFER
LOT 1: Operational gaps and overlaps on European level <i>Please provide your lump sum price for the total deliverables.</i>	P/Days	€
LOT 2: Proactive detection of network security incidents <i>Please provide your lump sum price for the total deliverables.</i>	P/Days	€
LOT 3: Secure communication with the CERTs and other stakeholders <i>Please provide your lump sum price for the total deliverables</i>	P/Days	€

Print name: <i>(of the Tenderer or authorised representative)</i>	Signature:	Date:
---	-------------------	--------------

ANNEX V

Model Service Contract template

(See attached file)

ANNEX VI

DECLARATION BY THE AUTHORISED REPRESENTATIVE(S):

NAME OF LEGAL REPRESENTATIVE	
<i>I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.</i>	
First name	
Last name	
Title (e.g. Dr, Mr, Mrs)	
Position (e.g. Manager, Director)	
Telephone number	
Fax number	
e-mail address	
Website	
NAME OF 2 nd LEGAL REPRESENTATIVE <i>(if applicable)</i>	
<i>I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.</i>	
First name	
Last name	
Title (e.g. Dr, Mr, Mrs)	
Position (e.g. Manager, Director)	
Telephone number	
Fax number	
e-mail address	
Website	

SIGNATURE: **DATE:**

ANNEX VII

Consortium form

Name of tenderer:

Form of the Consortium: (Please cross the relevant box)

Permanent: Legally established: Specifically for this tender:

	Name(s)	Address
Leader of the Consortium <i>(person authorised to conclude contract)</i>		
Partner 1*		
Partner 2*		

* add additional lines for partners if required. **Note that a subcontractor is not considered to be a partner.**

We confirm, as a partner in the consortium, that all partners are jointly and severally liable by law for the performance of the contract, that the leader is authorised to bind, and receive instructions for and on behalf of, each partner, that the performance of the contract, including payments, is the responsibility of the leader, and that all partners in the consortium are bound to remain in the consortia for the entire period of the contract's performance.

Signature: <i>Leader of consortium</i>	
Date:	
Signature: <i>Partner 1</i>	
Date:	
Signature: <i>Partner 2...etc</i>	
Date:	

ANNEX VIII

Sub-contractors form

	Name(s)	Address
Tenderer (person authorised to sign contract)		
Sub-contractor 1*		
Sub-contractor 2*		

* add additional lines for subcontractors if required.

As subcontractors for this tender, we confirm that we are willing to perform the tasks as specified in the tender documentation.

Signature: <i>Tenderer</i>	
Date:	
Signature: <i>Subcontractor 1</i>	
Date:	
Signature: <i>Subcontractor 2</i>	
Date:	

ANNEX IX Document CHECKLIST

WHAT MUST BE INCLUDED IN THE TENDER SUBMISSION:

PLEASE TICK EACH BOX AND **RETURN THIS CHECKLIST**

TOGETHER WITH YOUR OFFER

- | | | |
|----|---|--------------------------|
| 1 | Technical Offer | <input type="checkbox"/> |
| 2 | Professional information (<i>see Part 3 – Article 3.1</i>) | <input type="checkbox"/> |
| 3 | Proof of financial and economic capacity (<i>see Part 3 – Article 3.2</i>) | <input type="checkbox"/> |
| 4 | Proof of technical and professional capacity (<i>see Part 3 – Article 3.3</i>) | <input type="checkbox"/> |
| 5 | Legal Entity Form ⁶ (<i>Annex I</i>) <i>signed and dated</i> | <input type="checkbox"/> |
| 6 | Financial Identification Form ⁷ (<i>Annex II</i>) <i>signed and dated</i> | <input type="checkbox"/> |
| 7 | Declaration on Honour on exclusion criteria (<i>Annex III</i>) <i>signed and dated</i> | <input type="checkbox"/> |
| 8 | Financial Offer (<i>Annex IV</i>) <i>signed and dated</i> | <input type="checkbox"/> |
| 9 | Declaration by Authorised Representative (<i>Annex VI</i>) <i>signed and dated</i> | <input type="checkbox"/> |
| 10 | Consortium form (<i>Annex VII</i>) <i>signed and dated - if applicable</i> | <input type="checkbox"/> |
| 11 | Sub-Contractors form (<i>Annex VIII</i>) <i>signed and dated - if applicable</i> | <input type="checkbox"/> |

****The tenderers' attention is drawn to the fact that any total or partial omission of documentation requested may lead the Contracting Authority to exclude the tender from the rest of the procedure.***

Print name:

Signature:

Date:

(of the Tenderer or authorised representative)

⁶ If you have provided a Legal Entity form to ENISA within the previous 6 months maximum and no details have changed in the meantime, then you may provide a photocopy of this previous form.

⁷ If you have provided a Financial Identification form to ENISA within the previous 6 months maximum and no details have changed in the meantime, then you may provide a photocopy of this previous form.