



OPEN CALL FOR TENDERS

Tender Specifications

“Support and enhance cooperation between CERTs and with other communities”

ENISA P/01/12/TCD

LOT 1 - Good practice guides for CERTs in addressing operational and legal/regulatory NIS aspects of cybercrime

LOT 2 - Development and deployment of EISAS – pilot project

LOT 3 - CERT Inventory update & upgrade

- Part 1 Introduction to ENISA**
- 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. CONTEXT.....	5
1.1 Introduction.....	5
1.2 Scope.....	5
1.3 Objectives.....	5
2. ADDITIONAL INFORMATION.....	5
PART 2 TECHNICAL DESCRIPTION	6
A. THE PROGRAMME.....	6
B. SCOPE OF THIS TENDER.....	8
1 LOT 1: GOOD PRACTICE GUIDES FOR CERTS IN ADDRESSING OPERATIONAL AND LEGAL/REGULATORY NIS ASPECTS OF CYBERCRIME.	9
1.1 GENERAL DESCRIPTION OF THE REQUIRED SERVICES.....	9
1.2 OBJECTIVES AND TASKS.....	10
1.2.1 TASK 1: Development of the methodology.....	12
1.2.2 TASK 2: Data collection.....	13
1.2.3 TASK 3: Analysis.....	14
1.2.4 TASK 4: Compilation of the two good practice guides.....	15
1.2.5 TASK 5: Dissemination plan.....	16
1.2.6 TASK 6: Description of possible scenarios and topics for training as well as of possible usage of the two good practice guides for training.....	16
1.2.7 TASK 7: Project management.....	16
1.2.8 TASK 8: Handling input from possible ENISA 2012 informal Expert Groups.....	18
1.2.9 TASK 9: Assuring consistency between the two good practice guides and exploiting synergies during the data collection and compilation.....	18
1.3 EXPECTED SKILLS.....	18
1.4 DURATION.....	19
1.5 DELIVERABLES.....	20
1.6 DURATION OF THE SERVICE.....	22
1.7 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS.....	22
1.8 TENDER RESULT AND ESTIMATED CONTRACT VALUE.....	22
1.9 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER.....	23
2. LOT 2 - DEVELOPMENT AND DEPLOYMENT OF EISAS – PILOT PROJECT	24
2.1 EU POLICY CONTEXT.....	24
2.2 GENERAL DESCRIPTION OF THE REQUIRED SERVICES.....	26
2.3 OBJECTIVES AND TASKS.....	26
2.3.1 TASK 1: Preparatory phase - planning the pilot tasks.....	27
2.3.2 TASK 2: Implementation phase - Applying EISAS Basic Toolset methodology.....	28
2.3.3 TASK 3: Evaluation phase – Validate the feasibility.....	28
2.3.4 TASK 4: Draft the final report on the EISAS pilot.....	29
2.3.5 TASK 5: Prepare an enhanced roadmap for activities beyond 2012.....	29
2.3.6 TASK 6: Presentation of the results.....	29
2.3.7 TASK 7: Dissemination plan for external stakeholders.....	30
2.3.8 TASK 8: Project management.....	30
2.4 EXPECTED SKILLS.....	32
2.5 DURATION.....	32
2.6 DELIVERABLES.....	32
2.7 DURATION OF THE SERVICE.....	33
2.8 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS.....	33
2.9 TENDER RESULT AND ESTIMATED CONTRACT VALUE.....	34
2.10 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER.....	34

3.	LOT 3 - CERT INVENTORY UPDATE & UPGRADE	36
3.1	GENERAL DESCRIPTION OF THE REQUIRED SERVICES	36
3.2	OBJECTIVES AND TASKS	36
3.2.1	TASK 1: Review and update the Inventory document - focus on all CERT Teams in Europe	37
3.2.2	TASK 2: Review and update the Inventory document - focus on the national and governmental CERTs in Europe	37
3.2.3	TASK 3: Create an Europe CERT map	37
3.2.4	TASK 4: Presentation of the results	38
3.2.5	TASK 5: Project management	39
3.2.6	TASK 6: Dissemination plan for external stakeholders	40
3.3	EXPECTED SKILLS	40
3.4	DURATION	41
3.5	DELIVERABLES	41
3.6	DURATION OF THE SERVICE	41
3.7	PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS	41
3.8	TENDER RESULT AND ESTIMATED CONTRACT VALUE	42
3.9	CONTENT AND PRESENTATION OF THE TECHNICAL OFFER	42
4.	CONTENT AND PRESENTATION OF THE PRICE OFFER	44
5.	PRICE	44
6.	PRICE REVISION	44
7.	COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER	44
8.	PERIOD OF VALIDITY OF THE TENDER	44
9.	PROTOCOL ON PRIVILEGES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES	44
10.	PAYMENT ARRANGEMENTS	44
11.	CONTRACTUAL DETAILS	44
PART 3	ADMINISTRATIVE DETAILS	45
1.	FORMAL REQUIREMENTS	45
1.1	Address and deadline for submission of the Tender:	45
1.2	Presentation of the Offer and Packaging	46
1.3	Identification of the Tenderer	46
1.4	Participation of consortia	48
1.5	Subcontracting	48
1.4	Signatures of the Tender	49
1.5	Total fixed price	49
1.6	Language	49
1.7	Opening of the Tenders	49
2.	GROUND FOR EXCLUSION OF TENDERERS	49
2.1	Reasons for Exclusion	49
2.2	Other reasons for not awarding the Contract	50
2.3	Confidentiality and Public Access to Documents	50
3.	SELECTION CRITERIA	51
3.1	Professional Information	51
3.2	Financial and Economic Capacity	51
3.3	Technical and professional capacity	52
4.	AWARD CRITERIA	52
4.1	Quality of the Offer	52
4.2	Price of the Offer	53
5.	AWARD OF THE CONTRACT	54
6.	PAYMENT AND STANDARD CONTRACT	54
7.	VALIDITY	54
8.	LOTS	54
9.	ADDITIONAL PROVISIONS	54
10.	NO OBLIGATION TO AWARD THE CONTRACT	55
11.	DRAFT CONTRACT	55
12.	SPECIFIC INFORMATION	56

12.1 Timetable	56
ANNEX I	57
ANNEX II	58
ANNEX III	59
ANNEX IV	61
ANNEX V	62
ANNEX VI	63
ANNEX VII	64
ANNEX VIII	65
ANNEX IX Document CHECKLIST	66

PART 1 INTRODUCTION TO ENISA

1. CONTEXT

1.1 Introduction

ENISA, the European Network and Information Security Agency, is an Agency of the European Union (EU). It was set up to strengthen the capacity of the European Union, its Member States and the business community to prevent, address and respond to network and information security threats.

Computers and other information technology devices, such as smart phones, are now central to how Europe's citizens live their lives. Therefore, protecting digital information and networks is crucial, for society and the European economy.

In order to achieve this goal, ENISA acts as a centre of expertise in network and information security and facilitates cooperation between the public and private sectors. The Agency's mission is to support a high and effective level of Network and Information Security within the EU. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organizations in the European Union.

1.2 Scope

The Agency assists the Commission and the EU Member States, and cooperates with the business community in order to help them to meet the requirements of network and information security. This work supports the smooth functioning of the EU's internal market.

1.3 Objectives

The Agency's objectives are as follows:

- Advising and assisting the European Commission and the Member States on information security and in their dialogue with industry to address security 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 the Agency's capability to deal with information security threats.
- Awareness-raising and co-operation between different actors in the information security field, notably developing public and private sector partnerships with industry.

2. ADDITIONAL INFORMATION

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

PART 2 TECHNICAL DESCRIPTION

A. THE PROGRAMME

1. REINFORCING NATIONAL/GOVERNMENTAL CERTS

In its Communication on Critical Information Infrastructure Protection¹ 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 this 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)
- “take stock of the results of (pilot) projects and other national initiatives and to [...] further development and deployment of EISAS” (Chapter 5.2)
- “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”² 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)
- 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)
- highlights that *“Cooperation between CERTs and law enforcement agencies is essential [...]”* (Chapter 2.3)

In its Communication “The EU Internal Security Strategy in Action: Five steps towards a more secure Europe”³ the European Commission stresses ENISA’s role in improving Member States capabilities for dealing with cyber-attacks:

¹ “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

² “A Digital Agenda for Europe” (COM(2010) 245): http://ec.europa.eu/information_society/digital-agenda/index_en.htm

³ “The EU Internal Security 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, action 3). In this respect three discreet actions are quoted, being:

- *“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 has run a program dedicated to reinforce 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 practices 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;
- develops and deploys further the activities around information sharing and alerting of citizens in the Member States (EISAS).

One of the ENISA projects in 2011 was a good practice guide for CERTs in addressing NIS aspects of the fight against cybercrime⁴. Another ENISA deliverable in 2011 was a study on legal and regulatory aspects of information sharing and cross-border cooperation of

⁴ This report will be published in the ENISA website (at <http://www.enisa.europa.eu/act/cert/support>) or in any case made available to the contractor.

National/Governmental CERTs in Europe⁵. In addition, in 2011 ENISA organised together with Europol a workshop on CERTs and Law Enforcement Agencies (LEAs) addressing NIS aspects of cybercrime⁶.

The result of this Call for Tenders will follow up on previous activities in the field and will contribute to ENISAs CERT programme at large.

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 tender 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	Good practice guides for CERTs in addressing operational and legal/regulatory NIS aspects of cybercrime	€ 110,000.00
LOT 2	Development and deployment of EISAS – pilot project	€ 50,000.00
LOT 3	CERT Inventory update & upgrade	€ 10,000.00

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.

⁵ The study 'A flair for sharing – encouraging information exchange between CERTs - A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe' is available at <http://www.enisa.europa.eu/act/cert/support/legal-information-sharing>

⁶ More information about this event available at <http://www.enisa.europa.eu/act/cert/events/6th-workshop-cybercrime>

1 **LOT 1: GOOD PRACTICE GUIDES FOR CERTS IN ADDRESSING OPERATIONAL AND LEGAL/REGULATORY NIS ASPECTS OF CYBERCRIME.**

1.1 **GENERAL DESCRIPTION OF THE REQUIRED SERVICES**

In Chapter 2.3 of Communication “A Digital Agenda for Europe”⁷ 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 [...]”.

Responding to this requirement and following up on previous years activities, as foreseen in its 2012 Work Programme⁸ (WPK3.3: Support and enhance cooperation between CERTs, and with other communities), two of the ENISA activities in 2012 are:

- 1) to support national / governmental CERTs to help them in their cooperation with law enforcement, in order to contribute to vital and trusted information exchange, and to the establishment of a “well-functioning network of CERTs”. ENISA will also provide assistance regarding a system of contact points between CERTs and Law Enforcement Agencies (LEA), in order to help CERTs to play their part in prevention of cybercrime. An enhanced good practice guide for enabling CERTs to address technical NIS aspects of cybercrime in the form of a report is foreseen in this respect.
- 2) to further analyse legal challenges that CERTs in Europe might face when sharing information among them and provide possible solutions in dialogue with key stakeholders and to start exploring legal/regulatory and procedural obstacles faced by CERTs from Europe when cooperating and sharing information with CERTs and LEAs from Third Countries.

As for other activities these results shall contribute to ENISAs capability to make available sufficient training and exercise material for CERTs and the law enforcement communities.

The two expected deliverables from these activities are two good practices guides:

- 1) one good practice guide on operational NIS aspects of the fight against cybercrime; and
- 2) one good practice guide on legal/regulatory aspects of cybercrime.

The final aim of these activities and deliverables is to facilitate the work of CERTs and support their further improvement.

Possible operational NIS aspects of the fight against cybercrime might be:

- structured exchange of information on new cyber-attacks;
- digital forensics;
- assistance in cases requiring highly sophisticated digital evidence preservation.

The list is not exhaustive and is only indicative. Other operational NIS aspects should be identified during these activities.

⁷ “A Digital Agenda for Europe” (COM(2010) 245): http://ec.europa.eu/information_society/digital-agenda/index_en.htm

⁸ The ENISA Work Programme 2012 is available at <http://www.enisa.europa.eu/about-enisa/activities/programmes-reports>

Possible legal challenges to information sharing and cross border collaboration between CERTs and LEAs in Europe and CERT from Europe and CERT/LEAs of Third Countries might arise from:

- Definitions and criminal sanctions concerning different types of computer and network misuse;
- European legal framework governing data protection and privacy;
- Freedom of Information (Fol) and Public Sector Reuse of Information (PSI) legislation;
- Criminal procedure;
- Intellectual Property Rights;
- Confidentiality obligations;
- Determining applicable law.

The above list of potential legal challenges must be considered only as indicative and non-exhaustive.

Collecting data, analysing it, inventorying it and further processing it with a view to make reasonable suggestions, and compiling the two good practice guides in a consistent manner are necessary steps in the scope of this Call for Tenders.

The intended target audience for the good practice guide will be decision makers and experts at National/Governmental CERTs and other CERTs, policy makers in the Member States that are responsible for the integration of National/Governmental CERTs into the national cyber security strategy, LEAs. A discreet category of target audience of the good practice guide on legal/regulatory NIS aspects of cybercrime includes legal experts in the area of information security.

1.2 OBJECTIVES AND TASKS

With this Call for Tenders ENISA aims at collecting and analysing data concerning operational and legal/regulatory aspects.

For the good practice guide on operational NIS aspects of the fight against cybercrime, the focus should be on the operational, technical and practical barriers, challenges and incentives for the information sharing and cooperation of CERTs and LEAs in Europe. Best and good practices should be collected and recommendations should be made to improve the operational, technical and practical aspects CERTs are facing in their fight against cybercrime. Particular attention should be given to the cooperation between CERTs and LEAs, both on a national and international level, in this field and should give an overview as well of the current initiatives, organisations and cooperations active (in Europe) in the fight against cybercrime. The work done for this good practice guide should take into account the work done so far in this field and more specifically the recommendations and conclusions of the ENISA 2011 good practice guide for CERTs in addressing NIS aspects of the fight against cybercrime⁹.

⁹ This report is expected to be published in the ENISA website (at <http://www.enisa.europa.eu/act/cert/support>) and in any case made available to the contractor.

For the good practice guide on legal/regulatory NIS aspects of cybercrime, the focus should be:

- On the legal/regulatory and procedural challenges and the incentives for the information sharing and cooperation of CERTs and LEAs in Europe;
- On the legal/regulatory and procedural challenges and the incentives for the information sharing and the cooperation of CERT from Europe with CERTs and LEAs of Third Countries.

ENISA expects from the tenderer to include in the offer a project plan and a description of the methods proposed to achieve these expected results. The project plan requires a description of tasks to be carried out, a timeline with clear deadlines and frames for delivery of drafts and review (including peer-review), a description of deliverables, a list of potential parties to contact in order to collect ground information, a methodology for analysing data, a methodology for legal and regulatory research, a Gantt chart, and a quality assurance plan.

ENISA expects the tenderer to perform at least the tasks listed below. Details should be included as part of the offer. However, ENISA would consider any other proposal that adequately corresponds to the requested services.

Task 1: Development of the methodology

- a) Develop the most efficient methodology to identify stakeholders, to involve them, and to take into account their requirements
- b) Develop the most efficient methodology to collect the data

Task 2: Data collection

- c) Desktop research
- d) Online survey(s)
- e) Interviews

Task 3: Analysis

- f) Methodology for the analysis
- g) Definition of key concepts
- h) Identification of main stakeholders interacting with CERTs
- i) Description of the prevailing operational aspects
- j) Description of the prevailing legal and regulatory frameworks
- k) Inventory of operational barriers
- l) Inventory of legal and regulatory barriers, inventory of incentives
- m) Collection of existing good practices
- n) Analysis of the above (data, inventory etc.)

Task 4: Compilation of the two good practice guides

- o) Compilation of the good practice guides based on the data collected, including ENISA input and input from possible ENISA informal 2012 Expert Groups)
- p) Review cycle (including peer-review, review by possible ENISA informal 2012 Expert Groups and review by ENISA) as agreed with ENISA

- q) Presentation of the results in two good practice guides

Task 5: Dissemination plan

Task 6: Description of possible scenarios and topics for training as well as of possible usage of the two good practice guides for training

Task 7: Project management

- r) Timelines, deliverables, resources, quality assurance, Gantt chart, methodology etc.

Task 8: Handling input from possible ENISA informal 2012 Expert Groups

- s) Facilitating the collection
- t) Implementing the input

Task 9: Assuring consistency between the two good practice guides, exploiting synergies in the data collection and their compilation

Details of each task as it is expected by ENISA are given below.

1.2.1 TASK 1: Development of the methodology

This task is organised along the following main parts:

- Develop the most efficient methodology to identify stakeholders, involve them, and take into account their requirements
- Develop the most efficient methodology to collect the data

Details on the methodology and methods should be included as part of the offer.

ENISA expects the Tenderer to give details on the way stakeholders are identified, involved and their requirements are taken into account.

Concerning the methodology for the data collection, the Contractor is expected to collect data at least by carrying out a desktop research and through an online survey and interviews with key interviewees.

ENISA would consider any proposal on alternative/additional methodology to apply and alternative/additional methods to use.

Details on this methodology should be included in the offer.

Existing material (including but not limited to the 2011 ENISA report on cybercrime, 2011 ENISA study on legal and regulatory aspects of information exchange and cross-border cooperation of national/governmental CERTs in Europe, the outcome of the 2011 ENISA workshop on CERTs and LEA addressing NIS aspects of cybercrime, the ENISA documents on Baseline capabilities for National/Governmental CERTs¹⁰, the 'Legal Handbook for CSIRTs'¹¹, relevant European

¹⁰ Available at <http://www.enisa.europa.eu/act/cert/support/baseline-capabilities>

¹¹ Handbook of Legal Procedures of Computer and Network Misuse in EU Countries' available at: http://www.rand.org/pubs/technical_reports/TR337.html and the 'Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs' available at ftp://ftp.cordis.europa.eu/pub/isti/docs/directorate_d/trust-security/ec-csirt-d15.pdf

Commission funded projects, relevant policies papers, proposals for new legislation and regulation, and relevant ENISA material¹²) will be taken into account for this analysis.

Regarding the survey(s), the Contractor, in co-operation with ENISA and possible interaction with possible expert groups established by ENISA or some experts selected by ENISA, shall develop a structured survey capturing the key concepts, the operational barriers, the legal and regulatory frameworks, the legal and regulatory barriers as well as incentives, and possible solutions. The questionnaire might be validated by ENISA's experts and possibly by groups of experts selected by ENISA. The questionnaire(s) shall be developed by the Contractor taking into account the findings from the desktop research.

The Contractor will identify and submit to ENISA a list of interviewees (a minimum of three per country with an explanation on how the interviewees have been selected) before proceeding with the administration of the questionnaire(s)

1.2.2 TASK 2: Data collection

With regard to the good practice guide on operational NIS aspects, by using the most appropriate methodology, the Contractor is expected to collect data:

- 1) to define key concepts
- 2) to identify operational, technical and practical barriers, challenges and incentives for the information sharing and cooperation of CERTs and Law Enforcement Agencies (LEAs) in Europe;
- 3) to identify good and best practices in this domain;
- 4) to identify current initiatives, organisations and cooperations active (in Europe) in the fight against cybercrime.

This can be achieved, for example, through desktop research, online survey, interviews but also, for instance, with informal discussions with experts or internal knowledge/expertise.

With regard to the good practice guide on legal/regulatory NIS aspects, by using the most appropriate methodology, the Contractor is expected to collect data:

- 1) to define key concepts
- 2) to identify the legal and regulatory frameworks relevant for the information sharing of CERTs with LEAs in Europe and CERTs and other CERTs and LEAs from Third Countries;
- 3) to identify legal/regulatory and procedural challenges to collaboration and information sharing of CERTs-LEAs in Europe and CERTs-LEAs/other CERTs from Third Countries as well as incentives;
- 4) to identify possible solutions to the legal and regulatory challenges faced and, in order to reinforce the importance of cooperation.

¹² Main publications of ENISA available at: <http://www.enisa.europa.eu/publications>

This can be achieved, for example, through desktop research, online survey, interviews but also, for instance, with informal discussions with experts or internal knowledge/expertise.

1.2.3 TASK 3: Analysis

Having collected the information from the desktop research, the replies to questionnaire, the opinions expressed by key interviewees and experts (including ENISA experts and experts that ENISA might select for one or more expert groups), with the same degree of details for both the good practice guide on operational NIS aspects of cybercrime and the good practice guide on legal/operational regulatory NIS aspects of cybercrime, the Contractor is expected to carry out qualitative analysis of the data collecting in order for instance to:

- 1) Define key concepts
- 2) Identify main kind of interaction between CERTs and LEAs in Europe and CERTs and LEAs and other CERTs from Third Countries, e.g. kind of communication (face-to-face, secure email channels, informal information exchange, formal requests, etc.), the kind of information exchange, the information given each other, etc.
- 3) Describe the technical and legal/regulatory aspects of cybercrime
- 4) Compile an inventory of challenges and incentives
- 5) Compile an inventory of operational, legal/regulatory and procedural barriers and challenges and possible ways to overcome these challenges for the information sharing and cooperation of CERTs and LEAs in Europe
- 6) Collect existing good and best practices
- 7) Analyse the above (data, inventory, etc.), develop recommendations

The Contractor will propose a methodology for the analysis. The qualitative analysis should be carried out using a widely accepted method. It is expected that the Contractor will suggest a concrete method highlighting the importance and benefit of it to the project. The Contractor should also provide sufficient evidence of his/her expertise and knowledge of the proposed method.

The Contractor is expected to specify the necessary quality assurance methods and measures taken to ensure that stakeholders' input and contribution is taken properly under consideration and that the good practices adhere to their recommendations.

If during the analysis phase, it becomes evident that additional information is needed from specific experts, it is expected that the Contractor will either perform additional desktop research or contact the relevant expert(s) to obtain the required input.

The good practice guides should produce identification and definition of key concepts (e.g. categories and kind of data processed by CERTs, legal position of CERTs., digital forensics, sophisticated digital evidence preservation, etc.) and identification of the main subjects interrelating with CERTs and their legal and operational position.

The Contractor is expected to develop and describe the methodology used for analysing the data.

The Contractor is also expected to identify the relevant legal and regulatory framework and to compile an inventory of legal/regulatory and procedural barriers (grouped in categories) and operational, technical and practical barriers and challenges for the information sharing and

cooperation of CERTs and LEAs in Europe, and a list of ways to overcome these operational and legal challenges, an inventory of possible incentives. The study should also identify and present existing good practices in the field.

Based on the analysis of what described above (e.g. data collected, inventories, etc.) collected, the Contractor will develop recommendations for ENISA as well as other stakeholders, e.g. on how to contribute to overcoming the barriers. The recommendations should provide useful and practical advice to ENISA, CERT community, regulators and policy makers, law enforcement, etc. on how to improve their contribution to enhance the CERTs' co-operation in Europe and reduce barriers to information sharing and cooperation of CERTs and LEAs in Europe.

1.2.4 TASK 4: Compilation of the two good practice guides

The results of Task 3 (analysis, definition of key concepts, inventories, good practices and recommendations, etc.) will be included in two draft good practice guides that must be reviewed and validated by the Contractor in coordination with ENISA, also through a peer-review and possibly by informal Expert Groups to be established by ENISA in 2012.

After this, the Contractor is expected to update the good practice guide with the comments, suggestions and recommendations of ENISA and experts before issuing a final version.

The Contractor must ensure that a review of the two good practice guides is done before submitting it as final to ENISA. The offer must also contain a specific proposal for a peer-review and quality assurance.

The final product are two good practice guides, in other words two distinct and stand-alone but consistent documents that lays out the findings, the process that led to these suggestions, and present good practices in the field. One good practice guide will focus on the operational aspects, while the other on the legal/regulatory aspects.

The final deliverables must be provided to ENISA professionally proofread and with the ENISA layout implemented.

The final good practice guides might be published at ENISA's web site for open consultation. This way ENISA ensures that all possible stakeholders can suggest good practices and recommendations and make the good practice guide as inclusive and representative as possible. ENISA will finalise the good practice guide based on the additional comments received. ENISA retains the right to suspend the publication without justification and the right to update the good practice guide and issue new versions.

The two good practice guides should contain check lists, templates, graphs, thematic maps, tables and other graphical aids to help the reader to understand the results.

The two good practice guides must be written in English. The good practice guide focusing on legal/regulatory aspects must be understandable also by a person without a legal background. Legal and technical concepts must be expressed in an easy to understand manner.

In addition, the Contractor will provide a power point presentation as well as a proposal for a leaflet of:

- the good practice guide on operational NIS aspects of cybercrime;
- the good practice guide on legal/regulatory NIS aspects of cybercrime;
- both guides together.

All this material should be provided in an editable format easy to be updated by ENISA if necessary.

The Contractor will provide ENISA with raw data from the questionnaire/interview during the project implementation upon request and at the end of the project. ENISA might use this data for future activities.

1.2.5 TASK 5: Dissemination plan

The Contractor should report recommendations for the dissemination of the good practice guides, as an outcome of the questionnaire(s), to ENISA.

A document describing a dissemination approach for the two good practice guides, including channels and tools to use and a list of contacts will be compiled by the Contractor.

1.2.6 TASK 6: Description of possible scenarios and topics for training as well as of possible usage of the two good practice guides for training

The Contractor should identify possible scenarios (identified topics) and ways to use the material produced for training in the field of information sharing of CERTs.

A document identifying and describing which scenarios and topics and how the material produced could be used for training will be compiled by the Contractor.

1.2.7 TASK 7: Project management

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task the Contractor should also provide justification for subcontracting, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this report on budget.

The Contractor is expected to submit to the Agency, prior to the kick off meeting, detailed Gantt Charts and accompanying documentation with sufficient details. These will be negotiated with ENISA and be confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within the tasks
- Identification of milestones and critical activities
- Assignment of experts and person days to tasks and activities
- Identification of possible risks and suggestions to mitigate them
- Quality assurance and peer review measures to ensure high quality results
- Detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant projects,
- Detailed CVs of experts proposed to be involved in all the tasks of the project
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the
 - Tasks undertaken by the sub-contractor
 - Expertise of the contractor and its experts
 - Resources allocated to him/her
 - Co-ordination mechanisms among the prime and the sub-contractors
 - Risk management method in case of delayed and/or low quality delivery of sub-contractor's outcomes
 - Official statement of overall responsibility for the whole project and its results by the prime contractor
- Proposal for a peer-review

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief weekly progress report on current activities (as they defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, and risk mitigation measures
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision
- Minutes from the bi-weekly teleconferences with ENISA staff on the progress of the project and its tasks
- Intermediates and final reports on peer-review progress and quality assurance

In addition and on demand, the Contractor should be able to provide ENISA with a draft or snapshot of the results produced so far for the deliverables.

At least the following communication with the Contractor is expected:

- Four face-to-face meetings, whose at least one expected to be at ENISA's premises in Heraklion or at the ENISA Branch Office in Athens. Two other meetings are likely to be meetings with the informal Expert Groups that ENISA expects to establish in 2012 or ENISA workshops (these meetings will be maximum 1 day each and they will take place in a European city). A fourth meeting could be at the Contractor premises or at a place jointly decided by ENISA and the Contractor

- Regular video or teleconferences (bi-monthly or at more frequent intervals to be agreed upon) on the progress achieved
- At regular intervals or on an ad-hoc basis, as required, video or teleconference with the members of the informal Expert Groups that ENISA plans to establish
- At regular intervals or on an ad-hoc basis, as required, video or teleconference with the and with ENISA and the Contractor of a parallel related project that ENISA will carried out in 2012

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.

Informal and regular contacts should be maintained by telephone / Skype / Lync / video conferencing and e-mail.

1.2.8 TASK 8: Handling input from possible ENISA 2012 informal Expert Groups

This task relates to the facilitation of the collection and to the implementation of the input from the Expert Groups that ENISA plans to establish in 2012 to support the development and the review of the good practice guides.

The Contractor is expected to support the collection of the input from these Expert Groups and the implementation, including the compilation of documents showing how the comments from the Expert Groups are implemented.

Should a face-to-face meeting with the Expert Groups be organised, the Contractor is expected to support the preparation of the meeting in terms of, e.g. input to the agenda, preparation of presentation, participation and possibly presentation of intermediate and final results.

1.2.9 TASK 9: Assuring consistency between the two good practice guides and exploiting synergies during the data collection and compilation

While the two good practice guides will be two distinct and stand-alone documents, the Contractor will ensure consistency between them and will plan organise the data collection and their compilation in order to exploit synergies

1.3 EXPECTED SKILLS

The performance of the above mentioned activities requires professionals that have good academic, professional legal and multi-disciplinary knowledge on all of the following fields:

- Very good understanding of operational aspects the fight against cybercrime, both from the perspective of CERTs and LEAs at national and European level;

- Very good understanding of legal and regulatory as well as policy aspects related to CERTs and LEAs activities and information sharing at national, European, and international level;
- Very good knowledge of the work of CERTs, especially of:
 - incident handling service and its components
 - alerts & warnings service and its components
 - cooperation and information sharing among CERTs (especially during incident handling)
- Very good knowledge of LEAs and their activities, also at international level;
- Very good knowledge of the collaboration between CERTs and LEAs;
- Very good knowledge of cross-border information sharing also with Third Countries;
- Familiarity with CERT communities (FIRST, TF-CSIRT, etc.);
- Experience in carrying out research, analysing, and developing good practices and recommendations on relevant subjects;
- Very good knowledge of data collection and validation methods, including the ability to produce clear and understandable text;
- Experience in information security and CERTs issues, cross-border cooperation, information sharing, and relevant disciplines;
- Very good knowledge of data protection law, law regulating cross border collaboration and information sharing, service level agreements, intellectual property rights law, etc.
- Very good communication skills and in particular very good ability to express complex legal and/or technical concepts in a clear and easy to understand manner;
- Very good political acumen;
- Project management skills including quality assurance;
- Ability to use graphical aids (graphs, thematic maps, tables, etc.);
- Excellent oral and written language skills in English.

It is expected that possible tenderer may need to use the services of a subcontractor or to form a consortium in order to adequately cover all the specialised areas.

1.4 DURATION

The duration of this work is for around 5 months in the period May 2012 to end of September 2012. Please provide a suggestion for appropriate milestones and interim deliverables in your project plan (see article 1.9 below).

More specifically:

(where X = contract signature date):

- Task 1: (Development of the methodology) should be finalised not later than X + 1 months.
- Task 2: (Data collection) should be finalised by X + 3 months.
- Task 3: (Analysis) should be finalised not later than X + 4 months.
- Task 4: (Compilation of the two good practice guides) should be finalised not later than end of September 2012.
- Task 5: (Dissemination Plan) should be finalised no later than end of September 2012
- Task 6: (Description of possible scenarios and topics for training as well as of possible usage of the good practice guides for training) should be finalised no later than end of September 2012.
- Task 7: (Project Management) is an on-going task throughout this project.
- Task 9: (Handling the input from possible ENISA 2012 informal Expert) is an on-going task throughout this project.
- Task 9: (Assuring consistency between the two good practice guides and exploiting synergies during the data collection and compilation) is an on-going task throughout this project.

Please consider in your planning possible face-to-face meetings with the informal ENISA 2012 Expert Groups to gather and discuss their comments on draft good practice guide.

Please also indicate in your planning the time for the input and reviews by ENISA project teams, the time for input and review by the informal 2012 Expert Groups that ENISA plans to establish, the time for the final review by the ENISA management, and the time for implementation the implementation of the input and of the requested changes.

1.5 DELIVERABLES

The following deliverables are required from the Contractor:

D1: The questionnaire(s), the list of proposed questionnaire(s)' addressees and a suitable internet platform for the survey (linked to **Task 1**);

D2: Two reports (one for the operational aspects, one for the legal/regulatory aspects) on the results from the desk research as well as from the informal discussions with experts or internal knowledge/expertise

D3: Draft reports (one for the operational aspects, one for the legal/regulatory aspects) on main findings and analysis of them.

The draft report on operational aspects should include at least:

- 1) the replies to the questionnaire(s)
- 2) description of key concepts
- 3) inventory of barriers (with a focus on operational barriers) grouped by categories

- 4) inventory of incentives grouped by categories
- 5) existing good and best practices
- 6) detailed description of one issue (chosen based on the agreement with ENISA) identified during the research phase (including background information, motivation, detailed technical description of the issue, offered solutions and recommendation for an improvement in short-term with suggestions for concrete actions to take and stakeholders involved)
- 7) recommendations on how to overcome the barriers, with suggestions for concrete actions to take and stakeholders involved
- 8) possible recommendations from the respondents regarding dissemination of the report (linked to **Task 3**);
- 9) possible templates and check lists

The draft report on legal/regulatory aspects should include at least:

- 1) the replies to the questionnaire(s)
- 2) description of the legal and regulatory frameworks
- 3) inventory of barriers (with a focus on legal/regulatory and procedural barriers) grouped by categories
- 4) inventory of incentives grouped by categories
- 5) existing good practices
- 6) recommendations on how to overcome the barriers, with suggestions for concrete actions to take and stakeholders involved
- 7) possible recommendations from the respondents regarding dissemination of the report (linked to **Task 3**);
- 8) possible templates and check lists

D4: The two peer-reviewed final good practice guides (linked to **Task 4**)

D5: Power Point presentations on the final good practice guides (one for each guide and one for the two guides together) and proposal for leaflets (one for each guide and one for the two guides together) to marketing the good practice guide (linked to **Task 4**)

D6: Document describing a dissemination approach for the good practice guides, including channels and tools to use and a list of contacts (linked to **Task 5**)

D7: Document describing possible scenario and topics and possible usage of the good practice guides for training (linked to **Task 6**)

D8: Project plan and progress reports on predefined milestones (linked to **Task 7**)

D9: Document describing involvement and implementation of feedback of possible ENISA informal 2012 Expert Groups (linked to **Task 8**)

D10: Raw data (linked to Task 2)

The working language of the Agency is English. All documentation related to this activity is expected to be drafted in English, professionally proofread and presented by using the layout indicated by ENISA.

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.

- Four face-to-face meetings of one-day each (from 9:30 to 18:00); one meeting likely to be organised at ENISA premises in Heraklion or at the ENISA Branch Office in Athens (likely to be either a kick-off meeting or a progress meeting); two meetings likely to be with the informal Expert Group that ENISA plans to establish or ENISA workshops (these meetings will take place in a European city); one meeting is likely to be at the Contractor premises (likely to be a progress meeting) or at a place jointly decided by ENISA and the Contractor
- Regular video or teleconferences on the progress achieved (bi-monthly or at more frequent intervals to be agreed upon).
- At regular intervals or on an ad-hoc basis, as required, video or teleconference with the members of the informal Expert Group that ENISA plans to establish in 2012.

It should be mentioned that the costs of necessary business trips should be included in the Financial Offer (Annex I). ENISA will not additionally reimburse the Contractor for taking part in meetings or other events as outlined above.

Informal and regular contacts should be maintained by telephone / Skype / Lync / 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 for Lot 1. The total estimated budget cannot exceed **110,000.00 Euros (one hundred ten thousand Euros)**¹³ covering all tasks executed and including all costs (e.g. travelling expenses of the contractor etc.).

¹³ Please note that following implementation of the contract with the successful contractor and depending on the further needs of the contracting authority specifically in the field of endeavour the subject of this contract, the maximum amount contracted may be increased by up to 50% - subject to budget availability.

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 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
- 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 Contractor is expected to highlight / explain
 - Availability and ability of the Contractor to respond to ENISA request: 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.
 - If applicable, ability of the Contractor to manage services of a subcontractor or to work as a consortium in order to adequately cover all the specialised areas.
- 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 good practice guide.

2. LOT 2 - DEVELOPMENT AND DEPLOYMENT OF EISAS – PILOT PROJECT

2.1 EU POLICY CONTEXT

2.1.1 EISAS feasibility study

In its Communication (COM(2006) 251) the European Commission emphasized that public authorities in Member States and at EU-level play a key role in keeping citizens and SMEs properly informed¹⁴. In this way, they can contribute not only to their own safety and security, but also to a more resilient public communication infrastructure. The possibility of facilitating “effective responses to existing and emerging threats to electronic networks” should be explored.

In acknowledgement of these needs the European Commission requested ENISA to “examine the feasibility of a European Information Sharing and Alert System (EISAS)”, highlighting the role of ENISA in fostering a culture of network and information security in Europe. ENISA accepted this request and embarked on this study in 2006, which resulted in a report called *EISAS feasibility study – final report* (“the Feasibility Study”) that was published in 2007¹⁵.

2.1.2 EU Policy statements on National/Governmental CERTs and EISAS

In its **Communication on Critical Information Infrastructure Protection**¹⁶ 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 the same 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
- take stock of the results of (pilot) projects and other national initiatives and to further the development and deployment of EISAS.
- stimulate and support pan-European cooperation between national/governmental CERTs that should lead to enhanced preparedness, and
- to produce a roadmap to further the development and deployment of EISAS

¹⁴ A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”:
http://ec.europa.eu/information_society/doc/com2006251.pdf.

¹⁵ EISAS feasibility study – final report: <http://www.enisa.europa.eu/act/cert/other-work/eisas>.

¹⁶ “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

In its **Communication “A Digital Agenda for Europe”**¹⁷ 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”* and invites the Member States to act on this and; *“Establish by 2012 a well-functioning network of CERTs on national level covering all of Europe”*. (Chapter 2.3)

In its Communication **“The EU Internal Strategy in Action: Five steps towards a more secure Europe”**¹⁸, the European Commission emphasize the role of ENISA for the improvement of Member States capabilities for dealing with cyber-attacks. The European Commission anticipates the overall task for ENISA to “provide support to these actions with the aim of raising standards of CERTs in Europe.” In brief the three actions state that:

- Every Member State should have a well-functioning CERT,
- Member States should network together their national/governmental CERTs to enhance Europe’s preparedness.
- Member States together with ENISA should undertake regular exercises in incident response.

In the Communication, COM (2009)149, the EU Commission committed to support the development and deployment of EISAS by financially supporting two complementary prototyping projects (FISHA and NEISAS)¹⁹. In addition, the Commission also called upon ENISA “to produce a roadmap to further the development and deployment of EISAS”.

This roadmap was published in February 2011 and is entitled **“EISAS – European Information Sharing and Alert System for citizens and SMEs: A Roadmap for further development and deployment”** (“the EISAS roadmap”)²⁰.

2.1.3 ENISA’s program to reinforce CERTs

Since 2005 **ENISA runs a program dedicated to reinforce national/governmental CERTs**. The overarching goal is the proliferation of CERTs in Europe in general. In addition, there are multiple goals of this program:

- support the EU Member States to establish and develop 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 reinforce CERT operation and cooperation by making available good practice.

The result of this tender will contribute to ENISA’s program to reinforce CERTs²¹.

¹⁷ “A Digital Agenda for Europe” (COM(2010) 245):

http://ec.europa.eu/information_society/digital-agenda/index_en.htm

¹⁸ “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>

¹⁹ Critical Information Infrastructure Protection - a new initiative in 2009:

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

²⁰ EISAS – European Information Sharing and Alert System for citizens and SMEs: A Roadmap for further development and deployment:

http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

²¹ More details about ENISA’s program to reinforce CERTs, can be found at the ENISA website at this location:

<http://www.enisa.europa.eu/act/cert>

2.2 GENERAL DESCRIPTION OF THE REQUIRED SERVICES

2.2.1 Purpose

With this tender ENISA aim at procuring services for launching and coordinating a pilot of EISAS Basic Toolset deployment in one European Union Member State (EU MS) with support and cooperation of another EU MS.

In its Work Programme for 2012 (“WP2012”) ENISA included an activity, which is directly linked to the development of EISAS. This is laid out in Work Package (WPK) 3.3: “Support and enhance (co)operation between CERTs and with other communities”. This activity will focus on engaging MS and the national/governmental CERTs in implementing the EISAS roadmap produced in 2010. The roadmap lays out the way forward with the aim of deploying EISAS by 2013.

2.2.2 Goals

The goal of the general EISAS framework is to:

- **empower all EU citizens and SMEs** with the knowledge and skills necessary to protect their IT systems and information assets
- **build on national capabilities** of EU Member States, and
- **enhance cooperation** between national/governmental CERTs in the EU Member States

EISAS will be the result and the additional benefit gained from a reinforced cooperation between existing and to-be-built national capabilities.

2.2.3 Scope

The development and deployment of EISAS – as foreseen in the EISAS Roadmap – need to take into consideration “the findings from the EISAS Feasibility Study, the FISHA (NISHA) and NEISAS projects, and from other existing public and private initiatives”²². The results of the FISHA project and the goals of upcoming continuation of FISHA will play a role for the development and deployment of the EISAS Pilot.

2.3 OBJECTIVES AND TASKS

The main objective of this tender shall be to carry out a pilot for EISAS Basic Toolset 1.0²³ in one MS with the support of at least one another MS.

The objective is also to develop interconnectivity services between the participating organisations in the different MS and thereby paving the way for a full deployment of EISAS in 2013. The activity will also facilitate the development and/or improvement of National Information Sharing and Alert Systems (“ISAS”).

²² More information about FISHA and NEISAS can be found at the websites of the projects: <http://www.fisha-project.eu/> and <http://www.neisas.eu/>

²³ EISAS Basic Toolset report: http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas-basic-toolset

The intended target audience²⁴ for applying the EISAS Pilot will be those stakeholders who are foreseen to be involved in managing EISAS on the national level. Those are either national/governmental CERTs or other organisations/initiatives targeting citizens and SMEs.

The contractor is required to:

- Manage the EISAS pilot taking into consideration the outcomes of EISAS Basic Toolset 1.0, EISAS enhanced, EISAS feasibility study, FISHA project and EISAS Roadmap.
 - Identify the MS(s) willing to participate in this pilot together with its stakeholders
 - Involve n/g CERT and/or other NIS organizations who target the end users in the chosen MS(s)
 - Apply the methodology and approach of the EISAS Basic Toolset 1.0 (as a minimum, additional recommendations for an improvement can be suggested by and it is expected from the contractor)

Provide all necessary means, technology and information (e.g. the web survey tool) to be used for the EISAS Pilot project (as a minimum, but not limited to those used in the EISAS Basic Toolset 1.0)

- Coordinate all activities and participants in the preparatory, implementation and evaluation phases of the EISAS Pilot
- Analyse the results achieved
- Write a final report on the EISAS pilot project (including the evaluation of the used methodology, recommendation for an improvement in short-term with suggestions for concrete actions to take and stakeholders involved)
- Update EISAS roadmap
- Prepare a dissemination plan
- Provide a detailed project plan

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.

2.3.1 TASK 1: Preparatory phase - planning the pilot tasks

- The prospective contractor needs to identify stakeholders that will participate in the pilot (e.g. Member states, n/g CERT team or respective national initiative, potential participating companies and SMEs). In this regard the contractor needs to start with the list of MS and organisations willing to participate in this pilot which was already identified in the EISAS “enhanced” report.
- Research and identification of methods used by the concrete MS for citizens & SMEs security awareness.
- The contractor can adapt EISAS basic toolset according to the identified methods.(in coordination and agreement with ENISA)
- EISAS basic toolset approach is not exclusive; the contractor can come also with other suggestions or improvements which could be further approved by ENISA.

²⁴ For details see http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas-report-on-implementation-enhanced

- Likewise in the 'EISAS basic toolset' methodology the contractor must identify private sector companies, SMEs, and actively involve them in the pilot.
- As part of the cooperation component of the pilot project the prospective contractor must define a mechanism to (FISHA) obtain already validated information like good NIS practice guides from the more mature MS in awareness raising respect, and support the dissemination to other MS which runs the pilot. During the pilot, this mechanism must be tested between the MS.

2.3.2 TASK 2: Implementation phase - Applying EISAS Basic Toolset methodology

The contractor needs to coordinate start to end activities of the whole pilot project in each chosen MS. The method and the means of the coordination need to be explained in the offer.

- Awareness information needs to be disseminated with the help of n/g CERT teams and/or other national initiatives involved in awareness raising campaign targeting the end users and SMEs.
- Based on 'EISAS Basic toolset' methodology, the prospective contractor needs to use the suited channels for reaching citizens and SMEs with security awareness information.
- A web survey tool must be used for this task as a minimum. As part of applying the EISAS Basic Toolset, the contractor is expected to make sure that the materials used (ex. questionnaires, surveys or other ways proposed) are consistent in terms of content, style and language in all countries participating.

2.3.3 TASK 3: Evaluation phase – Validate the feasibility

- The contractor should define and set indicators to validate the overall effectiveness and usefulness of applying the EISAS Basic Toolset.
- As a minimum this validation should include indicators on:
 - Output (# of individuals targeted)
 - Outreach (# of individuals reached)
 - Impact (# of individuals taking which predefined desirable actions)
 - The contractor should make use of the questions in the Toolset
- The contractor is expected to tackle the challenges experienced during the validation of the Toolset as described in the EISAS Basic Toolset 1.0 report. Notably, increasing response rates among home users, at the same time ensuring anonymity for those respondents who so wish.
- The contractor should take note of identified risks, propose ways of how they could be realistically addressed, consider different types of incentives and assess the effect of these measures during the Validation phase.
- This task should partly be realised in cooperation with the MS representatives individually and/or as a workshop (usage of conference call technology possible; will be decided together with ENISA). It could be realised by, for example, desktop research, cost-benefit

analyses supplemented with input received from stakeholders (for example from the organisations with which the contractor intend to implement the EISAS Pilot).

2.3.4 TASK 4: Draft the final report on the EISAS pilot

The contractor is expected to include the result and conclusions of all previous tasks in the Final Report, in particular:

- Outcome of the application of the EISAS Basic Toolset
- Rationale behind the setting of goals and objectives for each of EISAS target group
- Reasons for the selection of security information material used in the intervention phase of the Toolset by the participating MS.
- Strategic advices/recommendations for the further development of EISAS Basic Toolset
- Detail the end-to-end methodology and approach used to obtain the results.
- Present the impact and effectiveness of the pilot.
- Short-term and long-term recommendations for improvement of EISAS Basic toolset

Follow-ups and actions concerning stakeholders involved in the pilot (ex. MS, n/g CERT, citizens & SMEs, companies) to run an efficient EISAS.

2.3.5 TASK 5: Prepare an enhanced roadmap for activities beyond 2012

- Based on results and outcome of the pilot, also taking into account the current EISAS Roadmap²⁵ and NISHA²⁶ (follow-up of FISHA) project, the prospective contractor must foresee the future activities of EISAS.
- Update the current roadmap with the identified activities taking in consideration a full deployment of EISAS in 2013 across MS.
- The contractor must also present the risks and concerns if any identified for a full deployment of EISAS and short/long term actions to overcome them.

2.3.6 TASK 6: Presentation of the results

The final products are one document with the report of the pilot and one document containing the updated roadmap.

The structure of both documents needs to be outlined in the offer (see section 'Content and presentation of the technical offer')

The layout of the final report of EISAS basic toolset pilot and the updated roadmap should be chosen to make possible updates of the content in the future easier.

²⁵ http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

²⁶ <http://fisha-project.eu/>

EISAS basic toolset pilot report must contain (but is not limited to):

- description of the work carried out and the impact of the results.
- description of the approach & methodology of the pilot.
- detailed description of each stakeholder role in the pilot.
- recommendation for improvement of EISAS basic toolset
- ENISA's role in this regard

EISAS roadmap document must contain (but is not limited to):

- Action plan for 2013 for a full deployment of EISAS taking into account the current roadmap.
- The risks and concerns related to the full deployment along with appropriate controls to overcome the risks

2.3.7 TASK 7: Dissemination plan for external stakeholders

- The Contractor should report recommendations for the dissemination of the enhanced roadmap and for the final report to ENISA.
- A document describing a dissemination approach for the two above mentioned documents including channels and tools to use and a list of contacts will be compiled by the Contractor.

2.3.8 TASK 8: Project management

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task the Contractor should also provide justification for subcontracting, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this pilot on budget.

The Contractor is expected to submit to the Agency, prior to the kick off meeting, detailed Gantt Charts and accompanying documentation with sufficient details. These will be negotiated with ENISA and be confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within the tasks
- Identification of milestones and critical activities
- Assignment of experts and person days to tasks and activities
- Identification of possible risks and suggestions to mitigate them
- Quality assurance and peer review measures to ensure high quality results

- Detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant projects,
- Detailed CVs of experts proposed to be involved in all the tasks of the project
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the
 - Tasks undertaken by the sub-contractor
 - Expertise of the contractor and its experts
 - Resources allocated to him/her
 - Co-ordination mechanisms among the prime and the sub-contractors
 - Risk management method in case of delayed and/or low quality delivery of sub-contractor's outcomes
 - Official statement of overall responsibility for the whole project and its results by the prime contractor
- Proposal for a peer-review

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief weekly progress report on current activities (as they defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, and risk mitigation measures
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision
- Minutes from the bi-weekly teleconferences with ENISA staff on the progress of the project and its tasks
- Intermediates and final reports on peer-review progress and quality assurance

In addition and on demand, the Contractor should be able to provide ENISA with a draft or snapshot of the results produced so far for the deliverables.

At least the following communication with the Contractor is expected:

- One kick-off meeting and one conclusion meeting in either one of the participating MS premises or at ENISA premises in Heraklion or at the ENISA Branch Office in Athens with the purpose of creating the synergies and set the basis for cooperation between MS in the pilot.

Regular video or teleconferences (bi-monthly or at more frequent intervals to be agreed upon) on the progress achieved

2.4 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 Information Security Management in general
- Very good understanding of the Human Factor aspects of Information Security
- Very good skills in designing and conducting surveys
- Experience in piloting ICT projects in the EU MS (cross-border management)
- Excellent project management skills including quality assurance
- Experience in carrying out research, analysing, and developing good practices and recommendations on relevant subjects;
- Experience in information security and CERTs issues, cross-border cooperation, information sharing, and relevant disciplines;
- Ability to use graphical aids (graphs, thematic maps, tables, etc.);
- Very good communication skills.
- Excellent oral and written language skills in English

2.5 DURATION

The duration of this work is foreseen between May and mid November 2012. Please provide a suggestion for appropriate milestones and interim deliverables in your project plan.

More specifically, assuming the Tasks described in article 'Objectives and Tasks' will be part of the final project plan (X = signing of the contract):

- Task 1, 2 should be finalised no later than X + 3 months
- Task 3,4 should be finalised no later than X + 6 months
- Task 5 should be finalised no later than end of October 2012.
- Task 6,7 should be finalised not later than mid-November 2012

2.6 DELIVERABLES

The following deliverables are required from the Contractor:

- Monthly progress report on predefined milestones
- **D1**: Intermediary report containing the planning phase and outcomes of Task 1
- **D2**: Intermediary report containing the survey materials, and IT Security information for awareness to citizens and SMEs
- **D3** Draft report containing the results of the pilot along with initial phases (Task 1, 2, 3)

- **D4** Final report document on EISAS pilot (Task 4) proof-read and imported into ENISA template
- **D5** Enhanced Roadmap document for 2013 and beyond (Task 5)
- **D6** PowerPoint presentation of the pilot and roadmap
- **D7** Dissemination plan
- **D8** Project plan and progress reports on predefined milestones
- **D9** Raw data from the surveys, and other materials used in the project

The working language of the Agency is English. All documentation related to this activity is expected to be drafted in English, professionally proofread and presented by using the layout indicated by ENISA.

2.7 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.

2.8 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 the Contractor's premises or even at a location convenient to both parties. The likely date for the kick off meeting will be defined within the second fortnight of May 2012.
- Regular teleconferences on the progress achieved (intervals to be agreed upon)

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.

Informal and regular contacts should be maintained by telephone / Skype / Lync / video conferencing and e-mail.

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.

2.9 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 **50,000.00 Euros (fifty thousand Euros)**²⁷ covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises).

2.10 CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information to enable the assessment of the offer 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 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 Article 6 entitled "Deliverables"
 - The requested proposals and additional details (see Article 6 "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
- 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 prospective contractor must also identify possible risks to the project and propose mitigation measures.
- In addition the tenderer 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.

²⁷ Please note that following implementation of the contract with the successful contractor and depending on the further needs of the contracting authority specifically in the field of endeavour the subject of this contract, the maximum amount contracted may be increased by up to 50% - subject to budget availability.

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

3. LOT 3 - CERT INVENTORY UPDATE & UPGRADE

3.1 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 2012 (WP2012) ENISA based on the work done in 2005 when an Inventory of CERT activities in Europe was developed will aim to produce with this tender a new and updated Inventory with all the European CERTs, their activities, existing cooperation between teams which in detail is laid out in Work Package (WPK) 3.1 of the WP2012.

The foreseen task in this WPK is a completely updated and extended “CERT Inventory”.

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

- have a full update of CERT teams in Europe
- have an inventory of activities , collaboration, initiatives between different teams interactive map of CERT teams across Europe

The expected result of the work of the prospective contractor is an inventory (including a text document, interactive maps to be embedded in ENISA’s website available also as a printable version, laying out the details and results of the tasks foreseen in the next section (please see also article “Objectives and tasks” for more details).

The intended target audience for this Inventory will be the CERT community, internet service providers, governmental institutions, private companies and internet security incident handlers from other sectors but not limited to the ones mentioned above.

3.2 OBJECTIVES AND TASKS

The prospective contractor will need to build upon the existing CERT Inventory²⁸ (web version & downloadable documents) and develop a comprehensive newly designed CERT Inventory document along with an interactive map of CERT teams in Europe with the emphasis on the national and governmental CERTs.

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 and offer an alternative approach how to achieve the same or better result:

²⁸ <http://www.enisa.europa.eu/act/cert/background/inv>

3.2.1 TASK 1: Review and update the Inventory document - focus on all CERT Teams in Europe

- identify new CERT Teams in Europe
- update the current information in the CERT inventory²⁹ document according to the new findings along with the basic contact details (in form of active links to their homepages if possible);
- update information regarding teams membership in the CERT communities like Trusted Introducer , FIRST;
- collect emails, PGP public keys & fingerprints of each CERT team;
- sort the identified CERT teams by the country and sector³⁰;
- research and verify current and identify new activities and collaboration initiatives among different CERT teams in EU –make a comprehensive overview;³¹
- The list of collected information it's not exclusive, the prospective contractor is expected to suggest other information that can be relevant.

3.2.2 TASK 2: Review and update the Inventory document - focus on the national and governmental CERTs in Europe

- Create a separate section for n/g CERT teams in Europe in the Inventory document.
- Research and identify all n/g CERTs in Europe and add them accordingly, to the new created section (ENISA can support the process based on its expertise)
- gather information regarding the hosting organization, sponsorship (funding), affiliation and the single contact point information (email and phone number) of CERT teams.
- add information regarding their membership in the CERT communities Trusted Introducer , FIRST and EGC (active links).
- collect PGP public keys & fingerprints of each n/g CERT team.
- research and identify all activities and collaboration initiatives among different n/g CERT teams in EU –make a comprehensive overview³²

3.2.3 TASK 3: Create an Europe CERT map

- create an interactive Europe map with all the CERT teams identified at TASK 1,2 for each European country (ex. Using technologies like Adobe Flash, HTML5+CSS, Google Maps API etc.).
- other technologies can be suggested by the contractor, with the observation that ENISA uses Plone/Zope CMS and the map must be fully integrated in the CMS.

²⁹ http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe/at_download/fullReport

³⁰ Besides the n/g CERTs which will be in a different section, all other teams can be classified by country/sector

³¹ See the section '**International CERT co-operation and initiatives inside and outside of Europe**' from CERT Inventory document available at the link from footnote 5

³² See the section '**International CERT co-operation and initiatives inside and outside of Europe**' from CERT Inventory document available at the link http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe/at_download/fullReport

- provide a functionality of displaying on the map only teams from a specific sector (ex. only n/g teams or only academic CERT, and/or all teams).
- create the possibility to hover over a specific country and click to find more details about the CERT teams in that specific country.(ex. Contact details: website, email etc or links pointing to country section on ENISA’s website³³)
- provide the capability to update the map. (ex. adding new CERT team on a specific country, update details of specific teams)
- create the possibility of printing the map (ex. print button), and downloading offline the map³⁴(see footnote for current approach) opting for all teams (in Europe, per country or per sector) and for n/g CERT only
- because of cross-browsing issues and different kinds of browsers and versions, the prospective contractor must provide fall-back mechanism for the map. (Ex. switching from HTML5 to HTML4 etc.)
- The above mentioned features are not exclusive, other improvements or suggestions for features from the prospective contractor are expected.
- Take appropriate security measures in the development of the application in order to protect against attacks like Cross-site Scripting XSS, DOM-XSS..

3.2.4 TASK 4: Presentation of the results

The final deliverable it’s a ‘CERT Inventory’ report and interactive map with CERT teams in Europe (n/g CERTs & others).

Its structure needs to be outlined in the offer (see article “Content and presentation of the technical offer”).

The layout of the final inventory (for all entries) should be chosen as to make possible updates of the content easier in the future. Improvements or suggestions for new layout are expected from the prospective contractor.

The ‘CERT Inventory’ report should contain:

- the inventory of all CERT teams across Europe.
- The new section dedicated to national/governmental CERTs
- the CERT teams listed in the report must have its afferent details (ex. Contact details (website, email etc.), sector & constituency, membership in Trusted Introducer or/and FIRST, PGP public keys and fingerprints)
- the n/g CERT teams must have its afferent details requested at TASK 2

The interactive map:

- Europe map with all the country members
- Hovering over a country will highlight that specific country
- Possibility of displaying and printing only the n/g CERTs and/or all CERTs of a specific country
- Clicking on the highlighted country will show more details regarding CERT teams in that specific country with links.

³³Please see <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

³⁴Please see <http://www.enisa.europa.eu/act/cert/background/inv/files/certs-in-europe-map>

- The interactive map must have the capability to update information, add new teams or/and change details for teams by ENISA experts (CMS based approach). (for printed and website versions)
- Presentation on the results with details explaining the interactive maps
- Written guidelines how to update the inventory and the maps (content and software wise)
 - Because of cross-browsing issues, different kinds of browsers and versions, the prospective contractor must provide fall-back for the map.

3.2.5 TASK 5: Project management

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task the Contractor should also provide justification for subcontracting, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this pilot on budget.

The Contractor is expected to submit to the Agency, prior to the kick off meeting, detailed Gantt Charts and accompanying documentation with sufficient details. These will be negotiated with ENISA and be confirmed as final.

The Gantt charts and related documentation should include:

- Scheduling of all tasks and activities within the tasks
- Identification of milestones and critical activities
- Assignment of experts and person days to tasks and activities
- Identification of possible risks and suggestions to mitigate them
- Quality assurance and peer review measures to ensure high quality results
- Detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant projects,
- Detailed CVs of experts proposed to be involved in all the tasks of the project
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the
 - Tasks undertaken by the sub-contractor
 - Expertise of the contractor and its experts
 - Resources allocated to him/her
 - Co-ordination mechanisms among the prime and the sub-contractors
 - Risk management method in case of delayed and/or low quality delivery of sub-contractor's outcomes

- Official statement of overall responsibility for the whole project and its results by the prime contractor
- Proposal for a peer-review

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief weekly progress report on current activities (as they defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, and risk mitigation measures
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision
- Minutes from the bi-weekly teleconferences with ENISA staff on the progress of the project and its tasks
- Intermediates and final reports on peer-review progress and quality assurance

In addition and on demand, the Contractor should be able to provide ENISA with a draft or snapshot of the results produced so far for the deliverables.

At least the following communication with the Contractor is expected:

Regular video or teleconferences via Skype, Lync (bi-monthly or at more frequent intervals to be agreed upon) on the progress achieved.

3.2.6 TASK 6: Dissemination plan for external stakeholders

- The Contractor should report recommendations for the dissemination of the Cert inventory document and map to ENISA.
- A document describing a dissemination approach for the two above mentioned documents including channels and tools to use and a list of contacts will be compiled by the Contractor

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:

- Very good ability to collect & analyse data.
- good IT skills – graphical website development skills
- Experience in web technologies like HTML5, CSS3, JavaScript, Ajax, Adobe Flash (ActionScript), Google Maps API, Plone CMS/Zope.
- Experience to draft concise reports on the European level
- Very good communication skills
- Excellent oral and written language skills in English

3.4 DURATION

The duration of this work is foreseen between May 2012 and end of August 2012.

More specifically, assuming the Tasks described in article “Objectives and Tasks” will be part of the final project plan (X = signing of the contract):

- Task 1 should be finalised not later than X + 2 months
- Task 2 and 3 should be finalised not later than X + 3 months
- Task 4 should be finalised not later than end of August 2012 with the complete final draft report available for the review by ENISA by August 20, 2012.

3.5 DELIVERABLES

The following deliverables are required from the prospective contractor:

- bi-weekly progress report on predefined milestones;
- D1 semi-final draft Inventory report + draft CERT map
- D2 Final CERT Inventory including all parts and EU Certs map (e.g. functional website and printable versions of the whole CERT inventory)
- D3 Project plan and progress reports on predefined milestones
- D4 PowerPoint presentation on CERT inventory, and map
- D5 Dissemination plan

*The CERT Inventory report must be proofread and adapted to ENISA’s template.

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.

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.

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 **10 000 Euros (ten 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).

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 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 tenderer 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.

The following specifications are common to ALL 3 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 **20 March 2012** 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 **20 March 2012** 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 despatch 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/01/12/TCD
“ Support and enhance cooperation between CERTs and with other communities ”
NOT TO BE OPENED BY THE MESSENGER/COURIER SERVICE
NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE 29th MAR 2012 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/01/12/TCD
“Support and enhance cooperation between CERTs and with other communities”
NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE 29th MAR 2012 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 **29th March 2012 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:

- a) Annual accounts, balance sheet or extracts from balance sheets for at least the last 2 years for which accounts have been closed, shall be presented where publication of the balance sheet is required under company law of the country in which the economic operator is established;

It is necessary that the extracts from balance sheets be dated, signed and stamped by the authorised representatives of the tenderer.

- b) 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.
- c) If tenderers will call on the competences of another entity (for example, a parent company), a written undertaking by the said entity certifying that it will make available to the tenderers the resources required to implement the contract.

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, following a request for clarification before the tender expiry date.

3.3 Technical and professional capacity

The following applies to LOTS 1, 2 and 3 identically:

Evidence of the technical and professional capacity of the tenderers shall be furnished on the basis of the following documents:

- A curriculum vita 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, Art 2.4 for LOT 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);
- 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	15/100
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 2.9 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

In case the successful tenderer is unable to sign the contract for any reasons, the Contracting Authority reserves the right to award the contract to other tenderers as per the ranking order established following the evaluation procedure.

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:** Good practice guides for CERTs in addressing operational and legal/regulatory NIS aspects of cybercrime.
- **LOT 2:** Development and deployment of EISAS – pilot project
- **LOT 3:** CERT Inventory update & upgrade

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 who's 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: **“Support and enhance cooperation between CERTs and with other communities”**

ENISA P/01/12/TCD

Summary timetable comments

Launch of tender - Contract notice to the Official Journal of the European Union (OJEU)	2 February 2012	
Deadline for request of information from ENISA	14 March 2012	
Last date on which clarifications are issued by ENISA	16 March 2012	
Deadline for submission of offers	20 March 2012	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	29 March 2012	At 10:00 Greek time
Date for evaluation of offers	29 March 2012	At 11:00 Greek time
Notification of award to the selected candidate	Mid April 2012	Estimated
14 day standstill period commences	Mid April 2012	Estimated
Contract signature	End April 2012	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

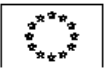
FINANCIAL IDENTIFICATION FORM

- 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:

“Support and enhance cooperation between CERTs and with other communities”

ENISA P/01/12/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: Good practice guides for CERTs in addressing operational and legal/regulatory NIS aspects of cybercrime. <i>Please provide your lump sum price for the total deliverables.</i>	P/Days	€
LOT 2: Development and deployment of EISAS – pilot project <i>Please provide your lump sum price for the total deliverables.</i>	P/Days	€
LOT 3: CERT Inventory update & upgrade <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 (for each LOT)**
- 2 **Professional information** (*see Part 3 – Article 3.1*)
- 3 **Proof of financial and economic capacity** (*see Part 3 – Article 3.2*)
- 4 **Proof of technical and professional capacity** (*see Part 3 – Article 3.3*)
- 5 **Legal Entity Form**³⁵ (*Annex I*) *signed and dated*
- 6 **Financial Identification Form**³⁶ (*Annex II*) *signed and dated*
- 7 **Declaration on Honour on exclusion criteria** (*Annex III*) *signed and dated*
- 8 **Financial Offer** (*Annex IV*) *signed and dated*
- 9 **Declaration by Authorised Representative** (*Annex VI*) *signed and dated*
- 10 **Consortium form** (*Annex VII*) *signed and dated - if applicable*
- 11 **Sub-Contractors form** (*Annex VIII*) *signed and dated - if applicable*

****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)

³⁵ 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.

³⁶ 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.