



## **OPEN CALL FOR TENDERS**

### ***Tender Specifications***

### **“Botnets: Detection, Measurement, Disinfection and Defence”**

**ENISA P/31/09/TSP**

**LOT 1 – Botnet Measurement Techniques;**

**LOT 2 - Detecting, Disinfecting and Defending against Botnets;**

**Part 1 Introduction**

**Part 2 Technical Description**

**Part 3 Administrative Details**

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

# CONTENTS

<b>PART 1 INTRODUCTION</b> .....	<b>4</b>
1.1. BACKGROUND .....	4
1.2. SCOPE .....	4
1.3. OBJECTIVES .....	4
1.4. TASKS.....	5
1.5. ORGANISATIONAL FRAMEWORK.....	5
1.6. ADDITIONAL INFORMATION.....	5
<b>PART 2 TECHNICAL DESCRIPTION</b> .....	<b>6</b>
2. GENERAL INTRODUCTION .....	6
2.1. The Resilience Program.....	6
2.2. Botnets .....	7
2.3. Requirements of the Study.....	8
3. SPECIFICATIONS for LOT 1.....	9
3.1. Measurement Techniques.....	9
3.2. Task 1 – Stock-Taking .....	9
3.3. Task 2 – Analysis, Good Practices and Recommendations .....	10
3.4. Task 3 – Project Management .....	10
3.5. Timeframe for provision of services.....	11
3.6. List of Outputs/Deliverables .....	12
3.7. Expected Skills.....	12
4. SPECIFICATIONS for LOT 2.....	13
4.1. Detecting, Disinfecting and Defending against Botnets .....	13
4.2. Task 1 – Identify Stakeholders, Stock Taking.....	13
4.3. Task 2 – Analysis, Good Practice Development and Recommendations.....	15
4.4. Task 3 – Project Management .....	16
4.5. Timeframe for provision of services.....	17
4.6. List of Outputs/Deliverables .....	18
4.7. Expected Skills.....	18
5. DURATION OF THE SERVICE .....	18
6. PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS.....	19
7. TENDER RESULT AND ESTIMATED CONTRACT VALUE .....	19
7.1. LOT 1 – Botnet Measurement Techniques.....	19
7.2. LOT 2 - Detecting, Disinfecting and Defending against Botnets .....	19
8. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER .....	19
9. CONTENT AND PRESENTATION OF THE PRICE OFFER.....	20
10. PRICE .....	20
11. PRICE REVISION .....	20
12. COSTS INVOLVED IN PREPARING AND SUBMITTING A TENDER.....	20
13. PERIOD OF VALIDITY OF THE TENDER.....	20
14. PROTOCOL ON PRIVILEGIES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES .....	20
15. PAYMENT ARRANGEMENTS .....	20
16. CONTRACTUAL DETAILS.....	20
<b>PART 3 ADMINISTRATIVE DETAILS</b> .....	<b>21</b>
1. FORMAL REQUIREMENTS.....	21
1.1 Address and deadline for submission of the Tender:.....	21
1.2 Presentation of the Offer and Packaging.....	22
1.3 Identification of the Tenderer.....	22
1.4 Participation of consortia.....	24
1.5 Subcontracting .....	24
1.4 Signatures of the Tender .....	25
1.5 Total fixed price.....	25
1.6 Language.....	25
1.7 Opening of the Tenders .....	25
2. GROUNDS FOR EXCLUSION OF TENDERERS .....	25
2.1 Reasons for Exclusion .....	25

2.2 Other reasons for not awarding the Contract.....	26
2.3 Confidentiality and Public Access to Documents.....	26
3. SELECTION CRITERIA.....	26
3.1 Professional Information .....	27
3.2 Financial and Economic Capacity .....	27
3.3 Technical Background.....	27
4. AWARD CRITERIA.....	27
4.1 Quality of the Offer.....	27
4.2 Price of the Offer.....	28
5. AWARD OF THE CONTRACT.....	29
6. PAYMENT AND STANDARD CONTRACT .....	29
7. VALIDITY.....	29
8. LOTS .....	30
9. ADDITIONAL PROVISIONS.....	30
10. NO OBLIGATION TO AWARD THE CONTRACT .....	30
11. DRAFT CONTRACT .....	30
12. SPECIFIC INFORMATION.....	31
12.1 Timetable .....	31
<b>CHECKLIST.....</b>	<b>32</b>
<b>ANNEX I.....</b>	<b>33</b>
<b>ANNEX II.....</b>	<b>34</b>
<b>ANNEX III.....</b>	<b>35</b>
<b>ANNEX IV .....</b>	<b>37</b>
<b>ANNEX V .....</b>	<b>38</b>
<b>ANNEX VI .....</b>	<b>39</b>
<b>ANNEX VII – Consortium form.....</b>	<b>40</b>
<b>ANNEX VIII – Sub-contractors form .....</b>	<b>41</b>

# PART 1 INTRODUCTION

## 1.1. BACKGROUND

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

For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises, and public sector organisations within the European Union (EU), thus contributing to the smooth functioning of the Internal Market, a European Network and Information Security Agency (ENISA) was established on 10 March 2004<sup>1</sup>.

## 1.2. SCOPE

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

## 1.3. OBJECTIVES

The Agency's objectives are as follows:

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

---

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

## 1.4. TASKS

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

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

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

## 1.5. ORGANISATIONAL FRAMEWORK

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

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

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

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

## 1.6. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: [www.enisa.europa.eu](http://www.enisa.europa.eu).

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

# PART 2 TECHNICAL DESCRIPTION

## 2. GENERAL INTRODUCTION

### 2.1. The Resilience Program

Reliable communications networks and services are now critical to public welfare and economic stability. Attacks on Internet, disruptions due to physical phenomena, software and hardware failures, and human error all affect the proper functioning of public eCommunications networks. Such disruptions reveal the increased dependency of our society on these networks and their services. This experience shows that neither single providers nor a country alone could effectively detect, prevent, and effectively respond to such threats.

The European Commission's Communications<sup>2</sup> have highlighted the importance of network and information security and resilience for the creation of a single European Information Space. They stress the importance of dialogue, partnership and empowerment of all stakeholders to properly address these threats.

The [existing](#) and recently proposed [updates](#) of Regulatory Framework Directives and the recent Commission's Communication on Critical Information Infrastructure Protection propose concrete policy and regulatory provisions for the improvement of the security and resiliency<sup>3</sup> of public e-Communications.

The European Network and Information Security Agency (ENISA), fully recognizing this problem, devised a Multi-annual Thematic Program ([MTP<sup>4</sup>](#)) with the ultimate objective to collectively evaluate and improve the resiliency of public eCommunications in Europe<sup>5</sup>.

In 2008 ENISA performed, inter alia, stock taking and analysis of Member States' (MS) policy, regulatory and operational environments related to the resilience of public eCommunications Networks. ENISA also performed a comprehensive analysis of provider measures.

The [stock taking](#) identified competent authorities at national level (stakeholders) and assessed their tasks, policies, initiatives, regulatory provisions and operational activities. Additionally, the activity also collected information at national level on information sharing between authorities and providers, national risk management processes, preparedness and recovery measures and other related issues.

The findings from the [analysis of the stock taking](#), [provider measures](#) and interaction with our stakeholders (12-13<sup>th</sup> of Nov. 08, [workshop](#), Brussels) revealed the importance of good practice guides on issues related to network security and resilience. According to the suggestions of

---

<sup>2</sup> “i2010 – A European Information Society for growth and employment<sup>2</sup>” & “A strategy for a Secure Information Society”,

<sup>3</sup> The ability of a network to provide and maintain an acceptable level of service in the face of various challenges to normal operation, ‘Stock Taking of Member States’ Policies and Regulations related to Resilience of public eCommunications Networks’, ENISA, 2008.

More information about MTP 1 can be found under:

[http://www.enisa.europa.eu/doc/pdf/management\\_board/decisions/enisa\\_wp\\_2008.pdf](http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf)

<sup>5</sup> [http://www.enisa.europa.eu/doc/pdf/management\\_board/decisions/enisa\\_wp\\_2008.pdf](http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf)

[Member States](#) and stakeholders, such guides could ideally be provided by a European body like ENISA on the basis of its own technical know-how.

In 2009 ENISA already started implementing this recommendation by developing three [good practice guides](#) on information sharing, incident reporting mechanisms, and resilience exercises.

In addition to the above topics, public and private stakeholders recommended ENISA to further analyse the availability and integrity of internet services, including critical ones. Attacks in both public and private provided services in [Estonia](#), [Georgia](#) but, also recently in US, UK and [South Korea](#) revealed the importance of Bot networks or Botnets in this area.

## 2.2. Botnets

Botnets are networks comprising computers infected by malicious code, or 'malware', which gives the people behind the botnets control over these computers to the extent that they can be used in a co-ordinated attack on a target.

The botnet owner can control unsuspecting users' infected computers via the botnet's command and control mechanisms, by connecting to bots via an IRC channel, a web connection, peer-to-peer networks or any other available means (even blog postings and Twitter posts have been reported). Estimates of average botnet size are in the 10's of thousands of machines but several have been detected with 100's of thousands. These are used to launch targeted attacks for extorting money or for political reasons.

Botnets cause business disruption, disruption of ordinary users' computers, network damage, information theft and harm to an organization's reputation.

- Administrators are often unaware that there is a botnet on their network until the organization is listed as a spammer on a domain name server block list.
- Botnets aggressively attempt to infect other computers in an organization.
- Confidential information such as client databases and bank account passwords are at risk of being stolen by the malware installed by botnets.
- The illegal actions of botnets damage the reputation, image and brand value of a business if it is seen as sending spam or facilitating other crimes.
- Botnets are often used to launch distributed denial of service (DDoS) attacks, where thousands of computers all access a website at once, overloading its servers and causing it to shut down.

Botnets have become a source of income for entire groups of cybercriminals and a vehicle for launching politically motivated targeted attacks. The low cost of maintaining a botnet and the ever diminishing degree of knowledge required to manage one are conducive to growth in popularity and, consequently, the number of botnets.

The cybercriminal's aim initially is to infect user machines with bot malware. This is done via drive-by infections in Web 2.0 sites by social engineering based on mass mailings, posting messages on user forums and social networking services or. Alternatively, the bot itself can self-replicate via viruses and worms. Various social engineering techniques are used for mass mailings or posting

messages on user forums and social networking services in order to cause potential victims to install a bot.

The [lease](#) of a mail botnet that can send about 1000 messages a minute (with 100 bots machines working online) costs about \$2000 per month. As in the case of leasing, the price of a ready-made botnet depends on the number of infected computers. Ready-made botnets are especially popular on English-speaking user forums. Small botnets of a few hundred bots cost \$200-700, with an average price amounting to \$0.50 per bot; Large botnets cost much more. Over the last few years botnets were successfully identified and neutralised. [Typical cases](#) are Storm, Conficker, Kraken, Szigbi, Bobax and others.

The spread of botnets is often presented as one of the biggest threats to Internet security. There are reports showing that several million computers are affected around the world. Several major security companies have reported information about the spread of botnets on a global level, but there is a lack of information about how these figures are established and the situation in Europe and/or individual countries.

Most stakeholders lack relevant statistics or are unable to break such data down to a national level. As virtually no Internet service providers are monitoring the spread of botnets, the information available largely consists of estimates. Most Internet service providers work preventively to help their customers avoid becoming affected by security problems. However, in relation to customers who are already infected, far from all Internet service providers take action to deal with the problem.

Already in 2007, ENISA performed a [small study](#) on [Botnets](#). The study mostly assessed the characteristics of botnets, the techniques used, the infection vectors of bots, the motivation of their creators and expected trends. The paper also identified roles and structures of criminal organizations for creating and controlling botnets (i.e. silent, 'hijacked' computers).

The study recommends that public and private stakeholders should better co-operate on policy, good practice and operational measures to combat botnets or reduce their impact. The study calls for continual effort rather than occasional inspections. It advocates that without help from users, combating botnets cannot be effective. Neglecting to stick to simple security rules can result in infected computers offering a backdoor to cybercriminals.

### 2.3. Requirements of the Study

This tender is organised into two lots:

- **LOT 1 – Botnet Measurement Techniques** - Stock-Taking, Analysis, Good Practices and Recommendations
- **LOT 2 - Detecting, Disinfecting and Defending against Botnets** - Stock taking, Analysis, Good Practices and Recommendations

Each LOT runs in an autonomous and independent way having its own management, resources and deadlines. The only dependency among LOTs is that the results of LOT 1 (good practices and recommendations on measurement techniques) will be validated by LOT 2 experts and stakeholders for transparency, openness and applicability purposes.

You may bid for **either** LOT 1 **or** LOT 2 **or for BOTH LOTS**. A separate service contract will be awarded for each LOT. In the event that the same tenderer is successful for both LOTs, then a consolidated service contract may be awarded.

### **3. SPECIFICATIONS for LOT 1**

#### **3.1. Measurement Techniques**

The objective of this LOT is to take stock of the techniques used for *measuring the extent* of botnets and their activities (i.e. the number and nature of infections) and to provide guidance on the best available measurement techniques and the limitations of techniques in use.

Understanding the nature of data available about botnets – its completeness and its accuracy or uncertainty - is an essential first step in responding to the threat they pose. Many figures on botnets are quoted without information on how they were arrived at or a quantitative analysis of the accuracy and completeness of the measurement methodology used. If the information is given, it often indicates a high degree of uncertainty. Yet many millions of Euros are being invested in the fight against botnets, on the basis of this information.

LOT 1 is organized into three tasks. Their requirements are given below.

#### **3.2. Task 1 – Stock-Taking**

The objective of this task is to collect information from leading experts and organisations in the field of botnet measurement with the following objectives:

- To understand what techniques are available to measure the size (number of bots), cost-per-bot, economic effectiveness (for the bot herder) and potential damage caused by existing botnets. Methods include for example, the use of honeypots, Sybil distribution on peer-to-peer networks, entropy based methods, statistical analysis, sensor networks, distributed honeybots, command and control based methods, etc...
- To understand for each technique, what are its technical strengths and weaknesses, known limiting factors, known areas of uncertainty in results and how its results compare with measurements of the same data by other techniques. The study should also examine legal implications of using various techniques (whether there are legal problems with using a certain technique in EU jurisdictions).
- To understand the relationship of measurement methods to categories of bots and methods of attack/disruptions.
- To identify which techniques are most commonly used in gathering data in Europe, giving examples of techniques used for data published about well-known botnets.

The contractor will identify prominent and relevant experts in the field of botnet measurement and collect information from them via:

- In-depth individual interviews and discussion (detailed objectives to be agreed with ENISA officer in advance) using electronic means (e.g. email, telephone, video conference, telephone conference) or physical meetings where appropriate. ENISA staff should be free to participate in telephone discussions.

- Group discussion among identified experts using electronic means. ENISA should be free to take part in this discussion.

If one physical meeting among the leading experts and ENISA's staff is needed to better pursue the objectives of this task, the contractor is expected to participate at their cost.

The contractor should provide to ENISA evidence of *at least 15* in-depth individual interviews and discussions with the above mentioned experts.

The contractor should also perform independent, desktop research of available material (e.g. relevant research and/or commercial projects, activities or initiatives at national, European, or global level projects).

### **3.3. Task 2 – Analysis, Good Practices and Recommendations**

The contractor will present the results of Task 1 in an easily digestible report where results for various available techniques can be easily compared.

This report will also:

- Analyse the strengths and weaknesses of the measurement methodologies identified in task 1
- Develop good practices of measurement techniques for different categories of botnets and stakeholders.
- Make Recommendations for a pan-European Strategy for effective, consistent and reliable measurement of Botnets across Europe

The report should clearly specify traceable sources for all information and well-reasoned argumentation for any judgements made. The report should clearly separate conclusions from any technical argumentation supporting them. This way the conclusions are understandable by non-technical readers.

This task should be carried out in close co-operation with the experts identified and be a consensus building exercise. In addition, the results (analysis, good practices and recommendations) will be presented for validation in a thematic workshop organised by ENISA.

ENISA will invite experts from different stakeholder categories to assess the quality of the findings and debate the proposed good practices and recommendations. The contractor is expected to present the findings and recommendations of this LOT to them during a validation workshop (expected in Sept or Oct of 2010).

### **3.4. Task 3 – 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 if required, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this study within the budget allocated.

The prospective contractor is expected to submit to the Agency detailed Gantt Charts and accompanying documentation with sufficient details including:

- 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

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

- Brief monthly progress report on current activities (as they are defined in the Gantt chart), information on the progress achieved, next steps, possible risks affecting project, 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.
- Bi weekly teleconferences with ENISA staff on the progress of the project and its tasks
- Participation in ENISA's thematic group of experts at regular or ad-hoc manner

ENISA expects that the prospective contractor will perform, in the context of this study, the following business trip:

- Kick off meeting: either at the contractor premises, at ENISA's or in a place jointly decided by ENISA and the contractor
- One physical meeting with the group of experts

It should be mentioned that the costs of such business trips should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in these meetings.

Prior to the kick off meeting, the prospective contractor is expected to submit detailed Gantt charts and relevant documentation. These will be negotiated with ENISA and be confirmed as final.

### **3.5. Timeframe for provision of services**

The duration of this work is foreseen between April 2009 and September 2010.

More specifically:

- Tasks 1 should start by April 1st 2010 and finish not later than end of July 2010

- Tasks 2 should start by April 1st 2010 and finish not later than end of September 2010
- Tasks 3 should start by April 1st 2010 and finish not later than end of September 2010

### **3.6. List of Outputs/Deliverables**

The following deliverables/outputs are required from the prospective contractor:

- Task 1 - Stock Taking – Delivery date 31<sup>st</sup> July 2010
  - List of experts contacted and their contact details
  - Questionnaire and results
  - Desktop Research results
- Task 2 - Analysis, Recommendations - Delivery date 30th September 2010
  - Analysis of Findings
  - Good Practices of Measurement Techniques
  - Recommendations for a pan-European Strategy for effective Measurement of Botnets
- Final Report – Botnet Measurement Techniques – Analysis, Good Practices and Recommendations - Delivery date 30th September 2010
- Professional Power Point presentation on the Final Deliverable - Delivery date 30th September

### **3.7. Expected Skills**

The performance of the abovementioned activities requires professionals that have good academic and professional multi disciplinary knowledge and experience of all or a sub set of the following fields:

- Proven professional and/or academic experience of measuring botnets at national and/or international level.
- Proven professional and/or academic experience of policies and measures related to botnets at national and/or international level.
- Good experience in organising stock taking exercises, analysis skills, and creating good practice guides and recommendations on relevant subjects.
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements;
- Good professional experience in relevant security issues and disciplines (e.g. antivirus software, DDoS, theft of confidential information, phishing, search engine spam, adware and malware);
- Good understanding of policy and regulatory issues related to the resilience of public eCommunications networks at national and/or pan European level including activities related to critical information infrastructure protection
- Excellent project management skills including quality assurance
- Very good communication skills.

## **4. SPECIFICATIONS for LOT 2**

### **4.1. Detecting, Disinfecting and Defending against Botnets**

The objective of this LOT is to take stock of and analyse policies, measures and methods to detect, disinfect and neutralise botnets. The analysis will enable the development of good practices and issuing of recommendations for all relevant stakeholders.

LOT 2 is organized into three tasks. Their requirements are given below.

### **4.2. Task 1 – Identify Stakeholders, Stock Taking**

This task is organised in three parts, namely:

- 1) Identifying relevant stakeholders
- 2) Comprehensive desktop research on relevant projects, initiatives, activities and studies in Europe and elsewhere.
- 3) Stock taking of detection, disinfection and defence methods, policies and measures

Concerning the first part, the prospective contractor should first identify relevant stakeholders and experts with significant experience and expertise in the above stated fields and engage their commitment to participate in the stock-taking exercise and following dialogue.

Typical categories of such stakeholders include

1. National and pan European Internet Service Providers (e.g. Telenor, Deutsche Telekom, France Telecom, Tiscali, Vodafone, etc.),
2. Antivirus software developers and security solutions providers (e.g. Symantec, ShadowServer Foundation, Kaspersky, Sophos, Aror Networks, S21 Sec, AhnLab, OpenDNS, etc)
3. Operating system providers (e.g. Microsoft)
4. Application and network providers and developers (e.g. Microsoft, HP, Cisco, etc.)
5. Web 2.0 and social network site providers (e.g. Google, You Tube, Twitter, FaceBook, etc.)
6. Academia (e.g. University of Manheim, FhG FIRST, IBM Watson Research Centre, Information Trust Institute at University of Illinois at Urbana-Champaign, etc.),
7. CERTs (e.g., FIRST, DFN Cert, US CERT, Swedish CERT, etc.),
8. Online user communities and consumer protection associations
9. Regulators and policy makers (e.g. PTS of Sweden, BSI of Germany, CPNI of UK, Ficora of Finland, EU Commission, etc.),
10. Law enforcement agencies (e.g. BKA of Germany, etc.),
11. Pan European Associations of Providers (e.g. EuroISPA, ETNO, Eco, Digital Europe, etc.).

ENISA will also mobilise its network of contacts and institutional bodies (i.e. PSG, MB and NLOs) to identify relevant experts that could possibly help the contractor to enrich his/her list of identified experts/stakeholders.

Concerning the second part, the prospective contractor is expected to identify and analyse relevant national, European, or global projects, activities or initiatives on botnet detection and disinfection, as well as, on policies and measures for defending against botnets. Such activities include academic and/or research-oriented projects but also commercial activities. The activities covered should not be restricted to technical measures, but should also include economic strategies and incentives, as well as co-operation initiatives among stakeholders. This can be

achieved through desktop research, web searching, informal discussions with experts, internal knowledge/expertise, and/or other possible means.

*ENISA will use all these contacts to form one or more virtual thematic group(s) of experts on relevant topics of the study.* Through the thematic group(s) of experts ENISA will engage the stakeholders in dialogue, sharing of information, identification of good practices and measures and development of recommendations for different categories of stakeholders. The prospective contractor is expected to electronically participate in the thematic group(s) and, in co-operation with ENISA, pursue the objectives and goals of the study. The contractor is expected to participate in one physical meeting of this group at their cost.

Concerning the third part, the prospective contractor, in co-operation with the ENISA and initial interaction with experts, will develop a questionnaire on the topics of the study, i.e. detection and disinfection, as well as policies and measures for combating botnets.

An *indicative* list of possible topics to be considered for both stock taking survey follows:

- Detection (but not measurement) methods at
  - ISP level (e.g. DNS traffic analysis),
  - Network level (e.g. malware detection)
  - Host Level (e.g. slow connection, strange browser behaviour, unknown network connections, etc.)
- Disinfection methods for both hosts, servers, C&C and networks
- Relationship of detection and disinfection methods to categories of bots and methods of attacks/disruptions,
- Measures for combating botnets for different categories of stakeholders at
  - technical level
  - organisational level
  - legal and regulatory level
  - dissemination and awareness level
  - economic/financial level
- Research issues and topics for detecting, disinfecting, measuring and defending botnets
- Barriers and obstacles for detecting, disinfecting, measuring and combating botnets,
- Good practices per category of bots and stakeholders for detecting, disinfecting, and combating botnets

The questionnaire will be used to collect input from all categories of stakeholders and experts mentioned above. The questionnaire will be validated by ENISA and a small group of relevant experts for its size, suitability and content. After the validation phase, the contractor will disseminate the questionnaire to the abovementioned stakeholders and follow up the process regularly so the return is maximised. After the collection of the replies, the prospective contractor is expected to carry out one-to-one interviews with selected stakeholders to further elaborate on the input received. The interviews will be done electronically, i.e. via telephone conferences.

ENISA will participate in all interviews to ensure the openness, transparency and quality of the process. The contractor is expected to summarise each interview in a written statement and seek validation by each group. If there are inconsistencies or incomplete answers the prospective

contractor is expected to repeat parts of the interview(s). A success indicator of this task is the number of participants, as well as the coverage of all potential public and private stakeholders.

ENISA will use the following three key performance indicators to ensure the quality and statistical value of the results:

- at least 10 replies for each category (1-11 above) of experts/stakeholders
- at least 4 interviews with each category (1-11 above) of stakeholders
- Returned questionnaires from ISP and service providers having leading market position in their country or at pan European level and representing in general 20% of the online user community in their markets

#### **4.3. Task 2 – Analysis, Good Practice Development and Recommendations**

In this Task the prospective tenderer is expected to

- Carry out qualitative analysis of the stock taking findings
- Develop appropriate good practices for detecting, disinfecting, measuring and combating botnets based on the analysis and the input received,
- Develop recommendations for different categories for stakeholders and propose follow up actions

The expected analysis should be carried out at two levels of abstraction.

- Analysis focusing on each topic of the questionnaire with the aim of identifying commonalities and differences among stakeholders' replies and contributions.
- Analysis focusing on groups of topics (aggregate analysis). The clustering of findings in groups should be done based on well defined criteria and jointly decided between the contractor and ENISA.

If during the analysis phase, it becomes evident that additional information is needed from specific stakeholders, it is expected that the prospective contractor will either perform additional desktop research or contact the relevant stakeholder(s) to seek the required input.

The qualitative analysis should be carried out using a widely accepted methodology that should be adequately explained as part of the application to tender in terms of benefits for this specific project. It is expected that the contractor will suggest a concrete methodology and also provide sufficient evidence of expertise and knowledge of it.

The prospective 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.

ENISA's experts will carefully follow up the analysis phase to ensure that all contributions from different stakeholders are properly and accurately taken into consideration.

Based on the analysis done, the prospective contractor is expected to develop good practices and draft recommendations for different categories of stakeholders.

The good practices should cover the following topics:

- Detection methods
- Disinfection methods
- Defence methods

The study should also propose recommendations for all categories of stakeholders. The recommendations should provide useful and practical advice to industry, academia, regulators, policy makers, law enforcement agencies and consumer organisations on how to improve their activities, enhance their co-operation, develop new measures and good practices, reduce barriers and develop, if needed, additional regulatory measures or interpretation of existing legislation.

The results of this LOT (i.e. analysis, good practices and recommendations) as well as the results of LOT 1 (i.e. analysis, good practices and recommendations) will be validated through experts and stakeholders in a thematic workshop organised and managed by ENISA.

ENISA will invite experts from different stakeholder categories to assess the quality of the findings and debate with us on the proposed good practices and recommendations. The workshop(s) will be organised and managed by ENISA. The contractor is expected to:

- Deliver to participants a draft version of the report three weeks before the validation workshop,
- Present the findings to them during the workshop,
- Collect input from participants,
- Prepare the minutes of the workshop
- Update the analysis report with participants' suggestions and reflections

The dates of the workshop will be agreed upon between ENISA and the contractor at the kick off meeting of the study. After the consultation workshop, the contractor is expected to update the report with the comments, suggestions and recommendations of stakeholders before issuing a final version of the report will be produced.

The final report with the analysis findings, good practices and recommendations will be published on ENISA's web site for open consultation. This way ENISA ensures that all possible stakeholders can suggest good practices and recommendations and make the report as inclusive and representative as possible. ENISA will finalise the report based on the additional comments received.

#### **4.4. Task 3 – 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. These will ensure the punctual delivery of good quality results of this study on budget.

The prospective contractor is expected to submit to the Agency detailed Gantt Charts and accompanying documentation with sufficient details for:

- 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

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

- Brief monthly progress report on running activities (as they defined in the Gantt chart) information on the progress achieved, next steps, possible risks affecting project, 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
- Bi weekly teleconferences with ENISA staff on the progress of the project and its tasks
- Participation in ENISA's thematic group of experts at regular or ad-hoc manner

ENISA expects that the prospective contractor will perform, in the context of this study, the following business trips:

- Kick off meeting: either at the contractor premises, at ENISA's or in a place jointly decided by ENISA and the contractor
- A thematic workshop organised and managed by ENISA to validate the good practices and recommendations of the study
- One physical meeting of the virtual group of experts

It should be mentioned that the costs of such business trips should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in these meetings.

Prior to the kick off meeting, the prospective contractor is expected to submit detailed Gantt charts and relevant documentation. These will be negotiated with ENISA and be confirmed as final.

#### **4.5. Timeframe for provision of services**

The duration of this work is foreseen between April 2010 and December 2010.

More specifically:

- Tasks 1 should start 1<sup>st</sup> of April 2010 and finish not later than end of August 2010
- Tasks 2 should start 1<sup>st</sup> of September 2010 and finish not later than December 1st 2010
- Tasks 3 should start 1<sup>st</sup> of April 2010 and finish not later than 1st December 2010

#### **4.6. List of Outputs/Deliverables**

The following deliverables/outputs are required from the prospective contractor:

- Task 1 - Identification of Stakeholders and Stock Taking – Delivery date 30<sup>th</sup> of August 2010
  - List of Stakeholders and Experts and their contact details.
  - Questionnaire and results
  - Desktop Research results
- Task 2 - Analysis, Good Practice Development and Recommendations – Delivery date 1<sup>st</sup> of December
  - Analysis of Findings
  - Good Practices for Detecting, Disinfecting, Combating botnets
  - Recommendations for different Categories of Stakeholders
- Final Deliverable - Botnets - Detection, Disinfection, Defence – Good Practices and Recommendations – Delivery date 1<sup>st</sup> of December
- Professional Power Point presentation on the Final Deliverable – Delivery date 31<sup>st</sup> of October
- Minutes of the validation workshops – Delivery date 1<sup>st</sup> of December

#### **4.7. Expected Skills**

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

- Proven professional and/or academic experience of detecting, disinfecting activities of botnets at national and international level
- Proven professional and/or academic experience on measuring botnets at national and/or international level
- Proven professional and/or academic experience on policies and measures combating botnets at national and international level
- Very good experience in organising stock takings and analysis on relevant subjects
- Very good understanding of policy and regulatory issues related to the resilience of public eCommunications networks at national and/or pan European level including activities related to critical information infrastructure protection
- Very good professional experience in relevant security issues and disciplines (e.g. antivirus software, DDoS, theft of confidential information, phishing, search engine spam, Adware and malware);
- Excellent data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements;
- Excellent project management skills including quality assurance
- Very good communication skills

#### **5. 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

clearly indicate the estimated amount of man days required to accomplish all tasks associated with this Call for Tenders.

## **6. 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.

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.

## **7. TENDER RESULT AND ESTIMATED CONTRACT VALUE**

The result of the evaluation of tenders will be the awarding of one Service Contract for each LOT. If the same tenderer is successful for both LOTs then one consolidated contract may be awarded.

### **7.1. LOT 1 – Botnet Measurement Techniques**

The total estimated budget for LOT 1 cannot exceed 40,000 Euros (forty thousand Euros) covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises).

### **7.2. LOT 2 - Detecting, Disinfecting and Defending against Botnets**

The total estimated budget for LOT 2 cannot exceed 80,000 Euros (eighty thousand Euros) covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises).

## **8. 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.

The Technical offer shall cover the following aspects:

- Description of the deliverables
- The deliverables must be presented as requested in article 3.6 for LOT 1 and article 4.6 for LOT 2.
- Management of provision of services
- Project Management: a close description of the project management method used including quality assurance is required.
- 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.

## 9. CONTENT AND PRESENTATION OF THE PRICE OFFER

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

## 10. 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.

## 11. PRICE REVISION

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

## 12. 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.

## 13. 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.

## 14. 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.

## 15. 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.

## 16. 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 **08 February 2010** either by:

- a) **Registered post.** Please note that **no offers by postal service will be accepted.**
- b) **Express courier.** The courier company printed delivery slip and stamp will constitute proof of compliance with the deadline given above:  
**or**
- c) **Hand-delivery** (direct or through any authorised representative of the Tenderer) by 17.00 hours on **08 February 2010** at the latest to the address shown below (please, be informed that only delivery during working hours 09:00-17:00 hrs, is accepted). In the case of hand-delivery, in order to establish proof of the date of deposit, the depositor will receive from an official at the below-mentioned address, a receipt which will be signed by both parties, dated and time stamped.

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

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

Postal Address		Express Courier & Hand Delivery
<b>Not applicable for this tender</b>	or	European Network and Information Security Agency (ENISA)  For the attention of Procurement Section Science and Technology Park of Crete (ITE) Vassilika Vouton 700 13 Heraklion Greece

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

## 1.2 Presentation of the Offer and Packaging

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

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

OPEN CALL FOR TENDER NO. <b>ENISA P/31/09/TSP</b>
<b>“Botnets: Detection, Measurement, Disinfection and Defence”</b>
NOT TO BE OPENED BY THE MESSENGER/COURIER SERVICE
NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE <b>16<sup>th</sup> FEB 2010</b>
TENDERED BY THE FIRM: <PLEASE INSERT NAME OF THE TENDERER/COMPANY>

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

OPEN CALL FOR TENDER NO. <b>ENISA P/31/09/TSP</b>
<b>“Botnets: Detection, Measurement, Disinfection and Defence”</b>
NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE <b>16<sup>th</sup> FEB 2010</b>
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, a company the following administrative information and documents must be provided (see administrative identification form attached as Annex I:

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 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 opening of received tenders will take place on **16<sup>th</sup> February 2010 at 10:00** at ENISA Building, Science and Technology Park of Crete, GR - 70013 Heraklion, Greece.

## **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;

- a. 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;

- b. Following another procurement procedure or grant award procedure financed by the Community budget, they have been declared to be in serious breach of contract for failure to comply with their contractual obligations.

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

## **2.2 Other reasons for not awarding the Contract**

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

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

See last paragraph point 2.1.

## **2.3 Confidentiality and Public Access to Documents**

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

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;
- Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

## **3. SELECTION CRITERIA**

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

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

### **3.1 Professional Information**

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

### **3.2 Financial and Economic Capacity**

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

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

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

### **3.3 Technical Background**

The prospective contractor should provide evidence (e.g. CVs of experts, previous projects in this field, references from customers, etc.) of expertise and knowledge on the topics mentioned below:

- experience incident reporting mechanisms and exercises related to the resilience of public eCommunications networks
- experience in organising stock taking and analysis in incident reporting and exercises
- understanding of national and pan European policies on incident reporting mechanisms and exercises
- experience in security issues and related disciplines (e.g. business continuity, crisis management, risk management/risk assessment, incident management);
- understanding of policy and regulatory issues related to the resilience of public eCommunications networks at national and/or pan European level;
- professional project management capabilities not only of national projects but also pan European ones

## **4. AWARD CRITERIA**

The following award criteria apply to both LOTS 1 and 2 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.	<b>Technical compliance</b>	Compliance with the technical descriptions (part 2 of this document)	30/100
2.	<b>Quality and accuracy of content and structure</b>	Quality of the proposal and accuracy of the description to provide the requested services	30/100
3.	<b>Project Team</b>	Composition of project team (ratio senior/juniors), work flows and review cycles of the output, direct involvement of senior staff, and distributions of tasks amongst experts; quality reviews of deliverables.	20/100
4.	<b>Methodology</b>	Selected survey methodology and project management	20/100
<b>Total Qualitative Points (QP)</b>			<b>100</b>

#### **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.

The offers exceeding the maximum price set in Part 2 Article 7 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 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:

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

Where;

- QP** = Qualitative points  
**PP** = Weighted price points  
**TWP** = Total weighted points score

## 6. PAYMENT AND STANDARD CONTRACT

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

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

## 7. VALIDITY

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

## 8. LOTS

This Tender is divided into Lots.

- **LOT 1 – Botnet Measurement Techniques** - Stock-Taking, Analysis, Good Practices and Recommendations
- **LOT 2 - Detecting, Disinfecting and Defending against Botnets** - Stock taking, Analysis, Good Practices and Recommendations

## 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. A draft copy of which is included as Annex V to this tender.

## 12. SPECIFIC INFORMATION

### 12.1 Timetable

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

Title: **“Botnets: Detection, Measurement, Disinfection and Defence”**

**ENISA P/31/09/TSP**

#### Summary timetable comments

Launch of tender - Contract notice to the Official Journal of the European Union (OJEU)	<b>18 December 2009</b>	
Deadline for request of information from ENISA	<b>02 February 2010</b>	
Last date on which clarifications are issued by ENISA	<b>04 February 2010</b>	
Deadline for submission of offers	<b>08 February 2010</b>	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	<b>16 February 2010</b>	At 10:00 Greek time
Date for evaluation of offers	<b>16 February 2010</b>	At 11:00 Greek time
Notification of award to the selected candidate	Late February 2010	Estimated
Contract signature (following '14 day standstill' period)	Mid March 2010	Estimated
Commencement date of activities	01 <sup>st</sup> April 2010	Estimated
Completion date of activities	December 2010	Estimated

## CHECKLIST

### WHAT MUST BE INCLUDED IN THE TENDER SUBMISSION:

PLEASE TICK EACH BOX  AND RETURN THIS CHECKLIST

TOGETHER WITH YOUR OFFER

1. Technical Offer
2. Legal Entity Form<sup>6</sup> (*Annex I*) dated and signed
3. Financial Identification Form<sup>7</sup> (*Annex II*) dated and signed
4. Declaration on Honour on exclusion criteria (*Annex III*) dated and signed
5. Financial Offer (*Annex IV*) dated and signed
6. Supporting documentation showing previous related experience  
as well as financial information and proof of registration
7. Declaration by Authorised Representative (*Annex VI*) dated and signed
8. Consortium form (*Annex VII*) dated and signed - if applicable
9. Sub-Contractors form (*Annex VIII*) dated and signed – 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.***

<sup>6</sup> 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.

<sup>7</sup> 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.

# ANNEX I

## Legal Entity Form

The specific form, for either a;

- d) public entity,
- e) private entity or
- f) 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](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 specimen, 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](http://ec.europa.eu/budget/execution/ftiers_en.htm)

	<b>FINANCIAL IDENTIFICATION</b>
PRIVACY STATEMENT	<a href="http://ec.europa.eu/budget/execution/ftiers_fr.htm">http://ec.europa.eu/budget/execution/ftiers_fr.htm</a>
<b>ACCOUNT NAME</b>	
ACCOUNT NAME <sup>(1)</sup>	<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"/>
<b>CONTACT</b>	
CONTACT	<input type="text"/>
TELEPHONE	<input type="text"/>
FAX	<input type="text"/>
E - MAIL	<input type="text"/>
<b>BANK</b>	
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 <sup>(2)</sup>	<input type="text"/>
REMARKS:	<input type="text"/>
<b>BANK STAMP + SIGNATURE OF BANK REPRESENTATIVE</b> (Both Obligatory) <sup>(3)</sup>	<b>DATE + SIGNATURE ACCOUNT HOLDER :</b> (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:**

- (a) 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;
- (b) has not been convicted of an offence concerning professional conduct by a judgment which has the force of res judicata;
- (c) has not been guilty of grave professional misconduct proven by any means which the contracting authorities can justify;
- (d) 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;

- (e) 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;
- (f) 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:

- (g) 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;
- (h) 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:

### “Botnets: Detection, Measurement, Disinfection and Defence”

#### ENISA P/31/09/TSP

Please provide your financial lump sum offer for **either** LOT 1 **or** LOT 2 **or for both** LOTS

<b>LOT Description:</b>	<b>Number of 'Man days' required for completion of project.</b>	<b>Your OFFER</b>
<b>LOT 1 – Botnet Measurement Techniques</b> <i>Please provide your lump sum price* for the total deliverables.</i>	M/Days	€
<b>LOT 2 - Detecting, Disinfecting and Defending against Botnets</b> <i>Please provide your lump sum price* for the total deliverables</i>	M/Days	€

\* Please note: This shall include all travel and subsistence costs associated with business trips as stated in the tender documentation.

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

# **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 <sup>nd</sup> 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
<b>Leader of the Consortium</b> <i>(person authorised to conclude contract)</i>		
<b>Partner 1*</b>		
<b>Partner 2*</b>		

\* 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.

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

## ANNEX VIII – Sub-contractors form

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

\* 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.

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