CLARIFICATION: N° 1

"Security and Resilience of electronic communications networks and services"

ENISA F-COD-13-T31

Questions & Answers

Q1:	**For LOT 1:** As the description "critical assets and services" is rather broad, an additional understanding of Enisa's interest in the focus and depth of this work is needed.
A1:	This is one of the objectives of the study: to identify what the critical components are, based on the desktop research, survey and interviews and draft an initial taxonomy. The depth of the work depends on the output of these steps. The goal is to have a categorization suitable for interested parties to use in everyday risk assessment. An example can be the connectivity links to ATMs.
Q2	**For LOT 1:** In particular, the following information would be helpful: a) The referenced document "Understanding the importance of Internet Infrastructure in Europe" b) Characteristic examples of "critical assets and services" in the focus of this call.
A2	a) Please find the document on the ENISA website; the URL is https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/guidelines-for-enhancing-the-resilience-of-ecommunication-networks b) Assets and services that are critical to the functioning of the society and if disrupted can have waterfall effects to the entire system and connected ones such as the connectivity links to ATMs.

Q3:	**For LOT 1:**
	
	Regarding Task 1 ("Stock taking")
	
	    a) EU MS efforts/initiatives as well as legal procurements for infrastructure security - does Enisa expect an exhaustive overview of those MS activities, even if they are not publicly documented or unavailable in English?
	
	    b) Interviews: What is meant by "7 different providers of critical services"? Are these IT-Service providers or other critical services like water-/power-suppliers, hospitals, fire workers etc.?
	
	    c) Interviews: What is the expected level of cooperation and support from Enisa during task 1? The reason for this question is that a high number (32) of interviews is requested with a concern of semi confidential information from public institutions (e.g., NRAs, cyber security agencies ...). On the very tight time scale, we envision little room for identifying and negotiating the willingness of institutions or responsible people to cooperate in the interviews.

A3:	a) It is duty of the contractor to collect all possible public information via desktop research and via confidential surveys and interviews.
	
	b) Yes, providers of critical services like water-/power-suppliers, hospitals, transport.
	
	c) The contractor in concert with ENISA is expected to define
	    - a list of possible stakeholders
	    - ad hoc confidentiality protocol (traffic light protocol)
	    - contents of the survey and the interview
	    - planning in line with the entire project
	The contractor is expected to organize surveys and interviews. ENISA will be present during the interviews and will supervise all the work.

Q4:	Concerning Part 3, Identification of the tenderer: 4) We, *<company name>*, are a BGB company under the civil code in *<country>*. According to the *<country>* law, we only had to register with the tax office, and are not obliged to publish a balance sheet. Correspondingly, we could provide (a) our constitutional contract, (b) registration with the tax office, and (c) tax assessment of the last two years. a) Would this satisfy the requirements of Part 3, Section 1.3?
A4:	In your particular case, the documents (a), (b) and (c) you have suggested should be sufficient, as long as the information regarding minimum turnover levels over the last 2 years can be established.