

**Statement for Stakeholder Meeting on the Availability and Robustness of
Electronic Communication Infrastructures – Brussels 18 June
By Marika Konings, Director European Affairs**

The Cyber Security Industry Alliance (CSIA) welcomes this opportunity to share its comments to the study commissioned by the European Commission on the availability and robustness of electronic communications infrastructures'. For those of you that do not know CSIA, CSIA is the only international industry association that is solely dedicated to cyber security policy issues. Our membership is composed of security hardware, software and services providers both from the United States and Europe.

Before going in to some specific points relating to the ten recommendations made by the study, I would like to briefly outline some general comments.

1. First of all, CSIA strongly believes in the value of public-private partnership to promote the robustness and resilience of critical information structures and we therefore welcome the efforts the Commission has taken to promote dialogue in this area.
2. Secondly, CSIA would like to point to other government related initiatives taken in this area such as the work undertaken by the IT Sector Coordinating Council, of which CSIA is a member, in the United States. Obviously we would not want to advocate a cut and paste approach, but we do believe valuable lessons can be learned from the good as well as the bad experiences of public – private cooperation in other parts of the world.
3. Thirdly, we would like to underline that the migration toward a truly converged ICT and the international make-up of the global networked infrastructures argue for involving global infrastructure companies in all aspects of planning, partnering and ICT protection.
4. Lastly, even though the study and recommendations are mainly focused on communication infrastructure and telecommunications in particular, CSIA encourages not to exclude the Internet as a special point of focus in the Commission's future CIP activities.

Now more specifically on the recommendations made by the study. In view of the limited time available I have picked out some of the main points of our paper related to specific recommendations, but I refer those of you interested in further details to the complete version.

Emergency Preparedness

CSIA agrees with the recommendation of convening a joint analysis group following emergency incidents as this could provide valuable information on if and how emergency

response planning would need to be adapted. In order not to duplicate such efforts, the European Commission could play an important role by providing a repository of information and promote the regular sharing of best and worst practices. For obvious reasons, information should be shared on a confidential, need to know basis only.

Confidential sharing of information is a key element of any partnership in this area. Equal partnership and a clear understanding of how information will be used, who will have access to it and for what purpose will help to create a basis of trust.

It is important to have 'Concept of Operations' documents in place which reflect the roles of all parties in the event of an emergency. The procedures which are documented in these CONOPS documents should be tested regularly by all participants.

Priority Communications on Public Networks

Communication capabilities in case of an emergency are key, not only for Member State governments and emergency services, but also for those industry players that have a crucial role to play in restoring critical communication infrastructures. In addition, it would be important to identify back up options that could be deployed, such as wireless and satellite in case it is not possible to access the standard public network, obviously with the appropriate security measures in place.

Critical Infrastructure Information Sharing

As mentioned before, secure, confidential sharing of information is key. An ideal or future state of information sharing should include policy, cultural, organisational and technological conditions that facilitate two-way, decentralised, yet coordinated information sharing. Information sharing should be understood as a broad concept, which embraces the trusted communication of many different types of information, having varying levels of sensitive and disclosure restraints, to trusted partners having specified responsibilities in CIP.

In this context, it might be worth pointing to the importance of sharing information on Internet related CIP threats, especially in view of the time sensitive nature these threats can have.

Supply chain integrity and trusted operation

Security software developers are committed to delivering software of the highest standards and substantial funds are spent on R&D to ensure that a product is robust and of high quality. The question is in the context of this recommendation, whether government institutions are the best placed to develop and oversee such an ambitious programme as proposed here. Furthermore, prescribing how integrity should be built into systems might have as an undesired side-effect limiting choice and innovation.

Unified European Voice in Standards

Enhanced international cooperation on the development of standards is desirable. However it needs to be taken into account that standards are there to improve quality, not to close off the market to third parties, which has happened in certain instances outside of the EU.

Vigorous ownership of partnering health

Many critical components of an available and robust ICT infrastructure are dependent on operational relationships: tangible, day-to-day information flows, acceptance of responsibilities and response/reconstitution actions that are embedded in the operational procedures of ICT stakeholder companies and government agencies. The health of this relationship should not be overlooked as it is crucial for the well-functioning of any public private partnership.

Discretionary European Expert Best Practices

There are numerous industry best practices that could serve as a useful tool or basis for further discussions. Two examples we mentioned in our paper are the Information Sharing and Analysis Centers Council Framework for Operational Information / Intelligence Sharing and the traffic light protocol (TLP) which was developed by the UK's National Infrastructure Security Co-ordination Centre.