



**Comments to Study on
Availability and
Robustness of Electronic
Communications
Infrastructures**

Final - May 2007

Introduction

The Cyber Security Industry Alliance (CSIA) welcomes this opportunity to provide its comments to the study commissioned by DG Information Society and Media on 'Availability and Robustness of Electronic Communications Infrastructures'. CSIA and its members have a long standing commitment and expertise in the area of critical information infrastructure protection stemming from hands on experience through its members' business activities as well as through its ongoing co-operation in this area with governments and other stakeholders. CSIA strongly believes in the value of public-private partnership to promote the robustness and resilience of critical information infrastructures which play such a crucial role in today's society.

Before providing specific comments to the 10 recommendations resulting from the study, CSIA would like to point to the initiatives undertaken in the United States by the IT Sector Coordinating Council (IT-SCC), of which CSIA is a member, in drafting the Information Technology Sector Specific Plan (SSP) in close co-operation with the US Department of Homeland Security. The draft IT-SSP is currently undergoing final revision and review by the Department of Homeland Security and other Departments of the US. Government. It details improvements for the enhancement of US capabilities for 1) prevention and protection through risk management, 2) situational awareness, and 3) response, recovery and reconstitution of information technology infrastructure. The final SSP is expected to be released shortly. Obviously, Europe's critical information infrastructures are not identical to those in the United States nor are the players involved, so we would not like to advocate a copy-paste approach. Nevertheless, there are many similarities, so we do hope good use will be made of the information and lessons learned in the US from the most comprehensive joint planning effort undertaken by the IT-Sector public-private security partners to date.

It is also worth pointing out that in the US, separate IT and Telecommunications SSP's were developed, but they were coordinated. The development process and the SSP's themselves reflect a deep understanding of the interdependency of government and the private sector in working to develop necessary public policy associated with ensuring the availability and robustness of ICT infrastructures. It has been a slow process, but in the US, there is now a greater appreciation today for the role of the private sector and the importance of including private sector entities in working with governments to assess risks, put into place appropriate controls, and be able to respond and reconstitute after major incidents. This is a difficult area, but an essential one.

As a general observation, CSIA would like to underline that the migration toward a truly converged ICT and the international make-up of the global networked infrastructure argue for involving global infrastructure companies in all aspects of planning, partnering and ICT protection. These infrastructures are global and do not stop at national or geographical borders. That understanding needs to be reflected in the steps taken by the European Commission in response to this study. Although many aspects of Europe's critical ICT infrastructure will be unique to Europe and the EU Member States, the underlying infrastructure in the IP-based network is a fabric involving private sector and government entities internationally. EU planning in response to the recommendations should reflect that reality, and those plans should include all major European and non-European companies who contribute to the hardware, software, and services making up the ICT infrastructure.

Furthermore, even though the study and recommendations are mainly focused on communication infrastructure, and telecommunications in particular, CSIA encourages the Commission not to exclude the Internet as a special point of focus in its future CIP activities and recommendations.

Also, we would like to re-emphasise our call to the Commission to include ICT as a priority sector in the implementation of the European Programme for Critical Infrastructure Protection (EPCIP) as outlined in our letter to Commissioner Viviane Reding and Commissioner Franco Frattini (see annex 1).

With regard to the study on 'Availability and Robustness of Electronic Communications Infrastructures', we have concentrated our comments on the 10 recommendations made the study as we understand these will be the main focus for follow up and next steps by the European Commission.

Recommendations

1. *Emergency Preparedness: "The private sector and Member State governments should jointly expand their use of emergency exercises and establish pre-arranged priority restoration procedures for critical services to better meet the challenges of inevitable incidents".*

Restoration of communication and information infrastructures is of critical importance in case of an incident or crisis. CSIA agrees that it is therefore crucial for the private sector as well as Member States to work better together to establish pre-arranged priority restoration procedures and expand the use of emergency exercises. However, there are a number of issues that would need to be addressed in order to do this in an efficient and co-operative manner.

- a) First of all, electronic communications networks are 'provided by a combination of entities – often owners and operators and their respective associations – that provide hardware, software, IT systems, and services. These entities maintain and reconstitute the network, including the Internet. The Internet encompasses the global infrastructure of packet-based networks and databases that use a common set of protocols to communicate. The networks are connected by various transports, and the availability of these networks and services is the collective responsibility of the IT and Communications Sectors.' It is therefore imperative to involve all stakeholders involved in this process if you want to create an efficient restoration procedure.
- b) The joint expansion of emergency exercises will require a substantial amount of investment both in time and money, especially in the case of exercises that cross different EU borders. The question is who bears the costs of these exercises?
- c) CSIA agrees that convening a joint analysis group following emergency incidents to study the response to incidents could provide valuable information on if and how the emergency response plan would need to be adapted. It would be important though that this information is shared with other stakeholders to avoid duplication and repetition of flaws. The European Commission could play an important role here 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.

- d) In this context, the flow of potential sensitive information is key to allow stakeholders to work together on an equal basis. A secure system for the sharing of confidential information will need to be developed in order to assure that all stakeholders feel comfortable in sharing sensitive information in a restricted setting. Another element that will play a role in the willingness to share information has to do with how sensitive the data is from a competitive perspective, or if it shows flaws in systems. Industry would want a clear understanding of how the info will be used, who will have access to it and for what purpose. Providing an incentive for stakeholders to participate, e.g. access to other useful data, might help.
- e) It is important to have “Concept of Operations” (CONOPS) 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 participants, both public and private sector, in addition to annual or ‘full-scale’ exercises which tend to be larger in scale and have cost implications.

A useful example might be the existing Telecommunications Priority Service plan in the US. Based on certain criteria, government and industry can designate certain critical telecommunications circuits that must be restored first, or in a pre-set sequence, in case of a significant outage. This is pre-designated, the US government approves the designations and special charges apply. In this way, no time is lost making these determinations in a crisis mode (see <http://tsp.ncs.gov> for further info). One should note that the issue of restoration after failure is one piece of the overall resiliency need. These vital communication circuits should also be engineered for maximum (reasonable) resiliency so that the likelihood of outage is reduced. In addition, one might need to consider the importance of identifying alternative facilities for essential circuits, like satellite or wireless.

2. *Priority Communications on Public Networks: “Member State governments should implement a standards-based priority communications capability for future public networks in order to ensure vital communications for critical government authorized callers. This public network capability is needed in addition to any private emergency networks that already exist and should not be viewed as a substitute or replacement for such private networks”.*

Communication capabilities in the 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. As mentioned before, it would be important to identify backup options that could be deployed, such as wireless and satellite, in case it is not possible to access the standard public network, with the appropriate security measures in place.

3. *Formal Mutual Aid Agreements: “The Private Sector should establish formal mutual aid agreements between industry stakeholders to enhance the robustness of Europe’s networks by bringing to bear the full capabilities of the European communications community to respond to crises”.*

There is no doubt that private sector stakeholders acknowledge and accept their reasonable responsibility for maintaining critical infrastructures, but it will be very difficult to translate this into legally binding mutual aid agreements due to a number of reasons such as different legal systems, question of costs involved, who concludes agreement with whom, under which jurisdiction, etc. Further discussion and research would need to be undertaken in order to translate this into a working practice at European level.

4. *Critical Infrastructure Information Sharing: “Member States and the Private Sector should establish formal means for sharing information that can improve the protection and rapid restoration of infrastructure critical to the reliability of communications within and throughout Europe”.*

As indicated before, sharing of information is crucial. Information sharing enables owners and operators, decision-makers, managers and others to detect, deter, and prevent attacks and incidents, identify trends, assess risks, provide warnings to help mitigate impacts and coordinate response activities. For information to be useful, it needs to be shared with the right people at the right time. 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. Without a trusted and effective information sharing infrastructure, other recommendations will not be achievable.

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. Taking into account the cross-border nature that is often inherent to Internet related CIP threats, it is of crucial importance to facilitate international intelligence sharing on an equal footing with partner networks and stakeholders. It is important to note that information sharing should not be viewed as a one way street but as a shared responsibility between all stakeholders involved.

5. *Inter-Infrastructure Dependency: “European Institutions and Member States should engage with the Private Sector to sponsor a coordinated European-wide program that identifies and addresses the interdependencies between the communications sector and other critical sectors, to enhance the availability and robustness of Europe’s public communications networks”.*

Especially in the case of critical information infrastructures, it is important to understand and assess the interdependencies that exist between sectors, but also the cross-border impact a potential incident can have. In addition, it is important that where critical interdependencies exist, proper risk assessment is carried out and lines of communication are put in place between those stakeholders involved in managing the infrastructures involved. Work in this area has been carried out at national level in a number of countries, so it might be worth looking at those examples that could serve as a potential model.

6. *Supply Chain Integrity and Trusted Operation: “European Institutions and Member States should embark on a focused program to promote the integrity of supply chains used to build network systems, and promote the implementation of innovative trust concepts to support the operation of these systems. The program should focus on articulating a vision, providing incentives for research and developments, and establishing policies affecting government procurement contract awards”.*

Security software developers are committed to delivering products of the highest standards. Substantial funds are spent on R & D to ensure that a product is robust and of high quality. In addition, international standards, such as the Common Criteria, provide assurances that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner. In this context, there are definitely areas for improvement such as the development of a common metrics to better measure quality and improve the current standardisation schemes. The question

is whether government institutions are the best placed to develop and oversee such an ambitious programme as proposed in this recommendation. Furthermore, prescribing how integrity should be built into systems might have as an undesired side-effect limiting choice and reducing innovation.

7. *Unified European Voice in Standards: “Member States should consider opportunities to coordinate positions during standards development, since multiple voices speaking in unison can give the European Union members more leverage in addressing concerns of mutual interest to the members. The Member States should coordinate the selection of standards bodies in which to actively participate. Member States should agree on which standards to follow to minimise conflicts”.*

From a European perspective, it would be helpful if Member States would coordinate positions during standards development as this would facilitate coming to a generally accepted approach. At the same time, the development of standards extends far beyond Europe and examples are known where regional / local standards are used as an excuse to exclude outsiders from participating in public tenders. Enhanced international co-operation on the development of standards is therefore desirable. Standards are there to improve quality, not to close off the market for third parties. Also, it needs to be taken into account that in a diverse area such as cyber security, a one-size-fits-all standard will not work and should not be the objective of such an initiative.

8. *Interoperability Testing: “The Private Sector and Member States should develop an industry-consensus, standardised, network-to-network testing framework to ensure a rigorous set of tests are performed prior to interconnecting new network to existing networks.*

Agreed, ensuring that the resilience and security, such as penetration and vulnerability testing, and risk assessment of the new network are also included in the testing framework.

9. *Vigorous Ownership of Partnering Health: “European Institutions, Member States and the Private Sector should re-invent their approach to collaborating and embrace a mind-set of unilateral responsibility for the success or failure of critical public-private partnerships”.*

Reinvention is not necessary in all cases, there are several examples where there are well functioning public-private partnership e.g. United Kingdom, but at the same time there are a number of European Member States where dialogue and co-operation is less well entrenched as an effective means to address critical information infrastructure protection. The most important elements of European public-private partnerships will be: equal partnership, sharing of information in a confidential but at the same time effective manner and a common agreed approach by all stakeholders.

In addition, 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 relationship.

10. *Discretionary European Expert Best Practices: “European Institutions and Member States should encourage the use of discretionary, industry-consensus Best Practices to promote the availability and robustness of Europe’s electronic communication*

networks. The Private Sector should contribute its expertise to industry Best Practice collaboration and implement the resulting Best Practices, where appropriate”.

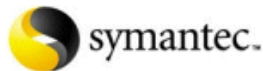
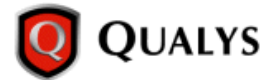
Definitely, there are industry best practices out there that could serve as a useful tool or basis for further discussions. As mentioned before, without a trusted and effective information sharing infrastructure, none of the recommendations will be achievable. In this context it might be worth pointing to the Information Sharing and Analysis Centers (ISAC) Council Framework for Operational Information / Intelligence Sharing (OIS). This framework identifies six components to information / intelligence sharing that must be addressed, and provides high-level approaches to addressing them. Its intent is to provide a usable and concise framework for use by CIP entities. The six components identified are:

- What is operational information / intelligence? – descriptions and definitions of information/intelligence sharing products
- With whom do we share operational information / intelligence? – entities and individuals who comprise the information/intelligence sharing infrastructure and their responsibilities
- How do we share operational information / intelligence? – the business processes and technical communications mechanisms used by information / intelligence sharing entities
- Originator control – a core component of the information / intelligence sharing process, addressing operational sharing policies and ground rules for voluntary sector and government sharing
- Vetting and trust – security and privacy guidelines needed to establish and maintain a trusted information / intelligence sharing environment
- Implementation – specific actions, responsible parties, deliverables, milestones and target dates needed to accomplish the goals of the framework

A similar paradigm exists in the United Kingdom, the so called “traffic light protocol” (TLP), which was developed by the National Infrastructure Security Co-ordination Centre (NISCC). Under the TLP the originator of the information labels it with one of four categories (indicated by different colours) to suggest further dissemination undertaken by the recipient (for example “no dissemination”, “limited distribution”, “community wide”, “unlimited”).

About CSIA¹

CSIA is an advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Launched in February 2004, its members include the leading cyber security software, hardware, and service companies. The organisation is led by CEOs from the world's top security providers, all international companies with a strong European presence. Its members include:



For further information, please contact

Tim Bennett
President, CSIA
2020 North 14th Street
Suite 750
Arlington, VA 22201
USA
Tel +1 703-894-1261
tbennett@csialliance.org

Marika Konings
Director of European Affairs, CSIA
Rond Point Schuman 6, box 5
1040, Brussels
Belgium
Tel +32 234 7850
mkonings@csialliance.org

¹ www.csialliance.org

Annex I

Commissioner Viviane Reding
DG Information Society and Media
B-1049 Brussels
Belgium

Brussels, 17 January 2007

RE: European Action Programme for Critical Infrastructure Protection

Dear Commissioner Reding,

On behalf of the Cyber Security Industry Alliance, I would like to applaud the European Commission for adopting its proposal for a directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. We believe this is an important step in mapping Europe's critical infrastructures as well as bringing together key public and private stakeholders to develop best practices and identify potential threats and weaknesses.

However, we strongly call upon the European Commission to include the ICT sector in its annual list of priority CIP sectors as its functioning, availability and restoration in case of an emergency or crisis is crucial to ensure the continued and efficient functioning of information technologies, infrastructures and services for people, businesses and government all across Europe. Virtually every other critical infrastructure sector, from energy to transportation, depends on the ICT sector to perform their most essential functions.

CSIA's members are committed to ensuring that critical cyber functions remain available, secure and resilient to meet the breadth of natural and man-made hazards that could disrupt the economy, threaten public health and safety or erode overall security. To this end, CSIA and its members have been working closely together with private and public partners. For example, CSIA has had a leadership role in the US IT-Sector Coordinating Council which has played an intrinsic part in developing the US IT Sector Specific Plan in close cooperation with the US Department of Homeland Security.

With this letter, CSIA and its members would like to share with you our commitment to work with the European Commission, the EU Member States and other stakeholders to share our expertise and know-how in this important area.

Yours sincerely,

Marika Konings
Director European Affairs

CC: Paola Colombo, Jacques Bus

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated exclusively to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Led by CEOs from the world's top security providers, CSIA believes a comprehensive approach to information system security is vital to the stability of the global economy. Visit our web site at www.csialliance.org.

Members of the CSIA include *Application Security, Inc.*; *CA, Inc.* (NYSE: CA); *BSI Management Systems*; *Citrix Systems, Inc.* (NASDAQ: CTXS); *Crossroads Systems, Inc.* (OTCBB Pink Sheets: CRDS.PK); *Entrust, Inc.* (NASDAQ: ENTU); *F-Secure Corporation* (HEX: FSC1V); *Fortinet, Inc.*; *Internet Security Systems Inc.* (NASDAQ: ISSX); *iPass Inc.* (NASDAQ: IPAS); *McAfee, Inc.* (NYSE: MFE); *Mirage Networks*; *MXI Security*; *PGP Corporation*; *Qualys, Inc.*; *RSA, The Security Division of EMC* (NYSE: EMC); *Secure Computing Corporation* (NASDAQ: SCUR); *Surety, Inc.*; *SurfControl Plc* (LSE: SRF); *Symantec Corporation* (NASDAQ: SYMC); *TechGuard Security, LLC*; and *Vontu, Inc*

Commissioner Franco Frattini
DG Freedom, Security and Justice
B-1049 Brussels
Belgium

Brussels, 17 January 2007

RE: European Action Programme for Critical Infrastructure Protection

Dear Commissioner Frattini,

On behalf of the Cyber Security Industry Alliance, I would like to applaud the European Commission for adopting its proposal for a directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. We believe this is an important step in mapping Europe's critical infrastructures as well as bringing together key public and private stakeholders to develop best practices and identify potential threats and weaknesses.

However, we strongly call upon the European Commission to include the ICT sector in its annual list of priority CIP sectors as its functioning, availability and restoration in case of an emergency or crisis is crucial to ensure the continued and efficient functioning of information technologies, infrastructures and services for people, businesses and government all across Europe. Virtually every other critical infrastructure sector, from energy to transportation, depends on the ICT sector to perform their most essential functions.

CSIA's members are committed to ensuring that critical cyber functions remain available, secure and resilient to meet the breadth of natural and man-made hazards that could

disrupt the economy, threaten public health and safety or erode overall security. To this end, CSIA and its members have been working closely together with private and public partners. For example, CSIA has had a leadership role in the US IT-Sector Coordinating Council which has played an intrinsic part in developing the US IT Sector Specific Plan in close cooperation with the US Department of Homeland Security.

With this letter, CSIA and its members would like to share with you our commitment to work with the European Commission, the EU Member States and other stakeholders to share our expertise and know-how in this important area.

Yours sincerely,

Marika Konings
Director European Affairs

CC: Lorenzo Salazar, Magnus Ovilius

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated exclusively to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Led by CEOs from the world's top security providers, CSIA believes a comprehensive approach to information system security is vital to the stability of the global economy. Visit our web site at www.csialliance.org.

Members of the CSIA include *Application Security, Inc.*; CA, Inc. (NYSE: CA); *BSI Management Systems*; *Citrix Systems, Inc.* (NASDAQ: CTXS); *Crossroads Systems, Inc.* (OTCBB Pink Sheets: CRDS.PK); *Entrust, Inc.* (NASDAQ: ENTU); *F-Secure Corporation* (HEX: FSC1V); *Fortinet, Inc.*; *Internet Security Systems Inc.* (NASDAQ: ISSX); *iPass Inc.* (NASDAQ: IPAS); *McAfee, Inc.* (NYSE: MFE); *Mirage Networks*; *MXI Security*; *PGP Corporation*; *Qualys, Inc.*; *RSA, The Security Division of EMC* (NYSE: EMC); *Secure Computing Corporation* (NASDAQ: SCUR); *Surety, Inc.*; *SurfControl Plc* (LSE: SRF); *Symantec Corporation* (NASDAQ: SYMC); *TechGuard Security, LLC*; and *Vontu, Inc*