FAQs to the report Good Practice Guide Network Security Information Exchanges

What is the background to this report?
This report is a part of ENISA's Multi-annual Thematic Program One (MTP 1), Resilience of Public e-Communication Networks. With this Program the Agency, among others, takes stock of and analyses Member States regulatory and policy environments related to resilience of public e-Communication Networks.

The report also contributes to European Commission (or EU) strategy of Critical Information Infrastructure Protection (CIIP)[1]. This strategy calls for wide deployment of national 'Network Security Information Exchanges' (NSIEs) and the creation of a pan European Public Private Partnership for Resilience. An NSIE is a form of strategic partnership among key public and private stakeholders aiming at sharing information on a particular field of discussion.

Member States are strongly interested in better understanding and deploying the concept of information sharing using an information exchange model. They requested ENISA to develop a good practice guide based on observed practices of existing information exchanges.

What is the aim of the guide?
The aim of this Guide, for those countries who do not operate an NSIE, is to assist network communication stakeholders and public bodies in national governments to set up and run an NSIE as a public/private sector partnership. For those countries, which already operate an NSIE, the aim is to provide an insight into other countries' good practice, to support continuous improvement and common approaches/practices.

A longer-term aim for this Guide is to support the development of common approaches and policies for information exchange and facilitate working relationships and understanding between each country's NSIEs. Hopefully the guide will also pave the way for an accelerated deployment of national NSIE and consequently of the establishment of a pan European information sharing platform.

How was this report conducted?
The content of the guide represents the aggregation of good practices from a number of countries having significant expertise and knowledge in the area and

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

individual discussions with experts. Additionally, the guide is based on a desk top research done for a number of non EU countries demonstrated expertise and knowledge in the area.

What does NSIE mean?

.

An NSIE is a form of a strategic partnership among key public and private stakeholders aiming at sharing information on threats, vulnerabilities and risks related to communication networks and their applications or services.

The drivers for this information exchange are the benefits of members working together on common problems and gaining access to information, which is not available from any other source. NSIE is an excellent vehicle to:

- better understand a changing security and resilience environment
- learn in a holistic manner about intrusions, vulnerabilities and threats
- develop recommendations for mitigating vulnerabilities, threats, & attack methods
- jointly develop methods to continuously assess existing measures
- provide unique insights and strategic views to policy makers and strategists.

What are the common characteristics of an NSIE?

The following list shows some of the common characteristics of an NSIE.

- The most effective size of a sharing group is between 20 and 30
- Regular, face-face meetings to establish and further enhance trust
- The Government's role is instrumental in setting up and running an NSIE together with industry
- An NSIE addresses strategic issues (e.g. major/critical disruptions) rather than operational ones
- Participation is free of charge
- New members require the unanimous agreement of existing members
- Most existing NSIE's are jointly chaired by a representative from the government and a representative from industry
- An NSIE should provide with incentives their members to participate
- An NSIE should respect members commercial sensitivities related to the disclosure of information to competitors and/or regulators
- Emphasis is on information exchange, not on information transfer
- High level security experts usually participate in NSIEs

What is really shared?
This is some of the information that is shared within an NSIE

- Experience and information on threats, risks, impact, vulnerabilities, incidents, counter measures
- Advisory support and warnings in implementing joint, sector wide, protective good practice measures
- Experience and information on:
  contingency planning
  crisis management
  analysis & mitigation of threats, risks, incidents, dependencies
- Information on emerging trends and changing environments
- Information on exercises, on methodologies and scenarios for conducting them.

How do you plan for and setup an NSIE?
For those new to NSIEs, a section in the report describes what an NSIE looks like in terms of its characteristics and features based on observed examples of NSIEs. Before looking in detail at good practice for setting up and running an NSIE, it is useful to look at the overall concept. At a high level, several NSIEs have drawn up mission statements with a view to specifying clearly and succinctly what the NSIE is and what it aspires to be. It is a good idea to involve as many stakeholders as possible in producing and refining the mission statement, and this helps develop a sense of ownership and responsibility.

With an understanding of the characteristics of an NSIE and an understanding of the environment in which it will operate, the report describes the specific elements of an NSIE, such as membership, building trust in an NSIE, focus on relevant value add services, interfaces with an NSIE, funding and costs, legal considerations and information inputs and outputs.

When you are convinced of the need for an NSIE, and you are aware of its vital components, you need to think about the practical strategies that you can use to get your NSIE up and running. One section in the reports looks at these strategies, which are presented as a set of action points.

Was there a need for a good practice guide?
ENISA's Resilience Program on the resilience of public e-Communication networks performed stock taking and analysis of Member States' policy and regulatory environments. The analysis of the stock taking findings revealed the importance of good practices in numerous areas including information sharing exchanges.

Information Exchanges is an under explored concept in Europe, as well as other parts of the world but countries that have long experience in this area strongly

recommend the establishment of such a strategic public private partnership with major stakeholders.

How is the guide structured?
Within the guide, issues and good practices are described within the various sections, using short quotes, presented in italics, from various sources to validate the points being made.

At suitable stages, observed good practices are highlighted to aid the reader of the guide make a choice whether the observed good practice is relevant to their own environment and need. These observed good practices are presented in a text box.

Who is this report for?
The main audience for this Guide is public and private sector stakeholders who operate and/or use communication networks and information systems and have responsibilities for infrastructure resilience matters.

Specifically, this guide will be useful for individuals and organisations who have an interest in setting up and running a Network Security Information Exchange, or who are looking for ways to enhance existing NSIEs.

For full report:
http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide

More information on the Resilience Program:
http://www.enisa.europa.eu/act/res

For further details, contact:
Dr. Vangelis OUZOUNIS, ENISA Senior Expert - IT Security Policies Technical Department, Evangelos.Ouzounis@enisa.europa.eu
Ulf Bergstrom, Press & Communications Officer ENISA, press@enisa.europa.eu, Mobile: +30 6948 460143