



EISAS – European Information Sharing and Alert System

A Feasibility Study

2006/2007



Table of Contents

1 EXECUTIVE SUMMARY	1
2 CONTEXT OF THIS STUDY	2
2.1 A SHORT HISTORY OF THE REQUEST TO ENISA	2
2.2 ABOUT ENISA	2
3 FORMAL PREREQUISITES (TERMS OF REFERENCE)	3
3.1 SCOPE AND OBJECTIVES	3
3.2 MOTIVATION – WHY HOME-USERS AND SMES?	3
3.3 METHODOLOGY OF THE FEASIBILITY STUDY	4
3.4 TIMELINE OF THE STUDY	4
4 PREPARATION OF THE STUDY – SETTING THE SCENE	5
4.1 AVAILABLE EXPERTISE IN ENISA	5
4.2 EWIS	5
4.3 ENISA STUDY ‘CERT CO-OPERATION AND ITS FURTHER FACILITATION’	8
4.4 ENISA INVENTORY OF CERT ACTIVITIES IN EUROPE	9
4.5 GAP ANALYSIS	9
5 GENERAL ASSUMPTIONS AND PRECONDITIONS	11
5.1 TYPES OF POTENTIAL ROLE FOR THE EUROPEAN UNION	11
5.2 BASIC COMPONENTS OF INFORMATION SHARING SYSTEMS	11
5.3 TYPES OF INFORMATION	12
5.4 THE DIFFERENT ASPECTS OF FEASIBILITY	13
5.5 POTENTIAL CANDIDATES FOR AN EXPERT GROUP	13
6 PHASE I: ANALYSIS OF THE CURRENT STATE OF AFFAIRS	14
6.1 ASSEMBLING THE EXPERT GROUP	14
6.2 ANALYSIS OF EXISTING SYSTEMS IN THE MEMBER STATES	15
6.3 INVENTORY OF PUBLICLY AVAILABLE SOURCES FOR NIS INFORMATION	29
6.4 THE WORKSHOP WITH THE EXPERT GROUP	31
6.5 CONCLUSIONS AND STARTING POINTS FOR PHASE II	31
7 PHASE II: EXAMINATION OF THE FEASIBILITY OF AN EISAS	33
7.1 INFORMATION GATHERING	33
7.2 INFORMATION PROCESSING	34
7.3 INFORMATION DISSEMINATION	36
7.4 CONCLUSIONS	38
7.5 PROPOSED SCENARIO	39
7.6 STARTING POINT FOR PHASE III	41
8 PHASE III: ASSESSMENT OF THE ADDED VALUE	42
8.1 ACT AS A CLEARING HOUSE FOR GOOD PRACTICE FOR NATIONAL ISASS	42
8.2 SUPPORT NEW NATIONAL ISASS	42
8.3 FOSTER DIALOGUE AMONG EXISTING NATIONAL ISASS	42
8.4 ANALYSE AND REVIEW PRACTICE, COMPONENTS AND PROCESSES TO OPTIMISE INFORMATION SHARING FOR THE EXISTING (N)ISASS	43
8.5 PROPOSAL OF INDICATORS	43
9 PROPOSED NEXT STEPS	45
9.1 START SMALL, BUT THINK BIG	45
9.2 PROOF OF CONCEPT	45
9.3 THE POTENTIAL ROLE OF ENISA	48
ANNEX A: THE TERMS OF REFERENCE	51
ANNEX B: INVENTORY OF SYSTEMS	53
ANNEX C: INVENTORY OF PUBLICLY AVAILABLE SOURCES	57
ANNEX D: MINUTES OF THE MEETING OF THE EXPERT GROUP	63
ANNEX E: TIMELINE OF THE STUDY	67
ANNEX F: SAMPLE PRESENTATION ABOUT THE FEASIBILITY STUDY	68
ANNEX G: TERMS AND DEFINITIONS	71

1 Executive Summary

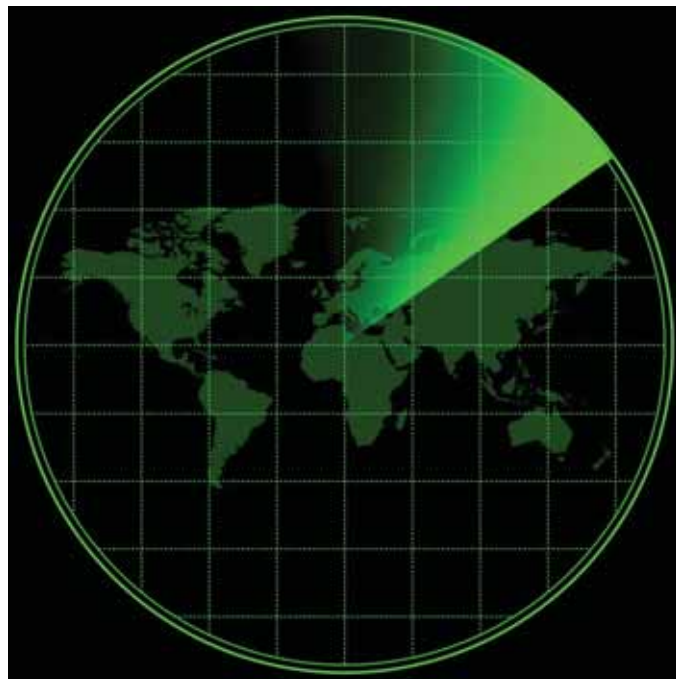
There are many systems and initiatives across Europe that have the goal of disseminating appropriate and timely information on Network and Information Security (NIS) vulnerabilities, threats, risks and alerts, as well as sharing good practices. ENISA was asked to analyse the current state of affairs as regards such systems and initiatives in the public and the private sectors in the EU Member States and to identify possible sources of security information that could potentially contribute to a Europe-wide Information-Sharing and Alert System (EISAS).

It was hoped that the findings of this analysis would lead to the development of a scenario that would both address the lack of available NIS information in some Member States and add value (in a way yet to be determined) to existing information sharing systems in other Member States. Ideally such an EISAS would build on these existing systems, firstly to avoid the duplication of effort and competition, and secondly to draw from the lessons learned and the good practices of these (national) systems.

In defining the most promising scenario for a European involvement in this field, the study analysed first the findings of previous projects and other studies with a similar scope and second the status quo of the existing (national) information sharing systems for home-users and Small and Medium Enterprises (SMEs).

Two types of involvement for the European Union (operating and facilitating) in the three parts of the information sharing process (information gathering, processing and dissemination) have been examined under three different perspectives (technical/organisational, political and social/cultural).

The study concludes that the most effective level of involvement for the European Union in the establishment and operation of an information sharing system for its home-users and SMEs would be that of a facilitator, moderator of discussion and a 'keeper of good practice'. The report closes with proposals for the next steps to be taken and a 'proof of concept' scenario.

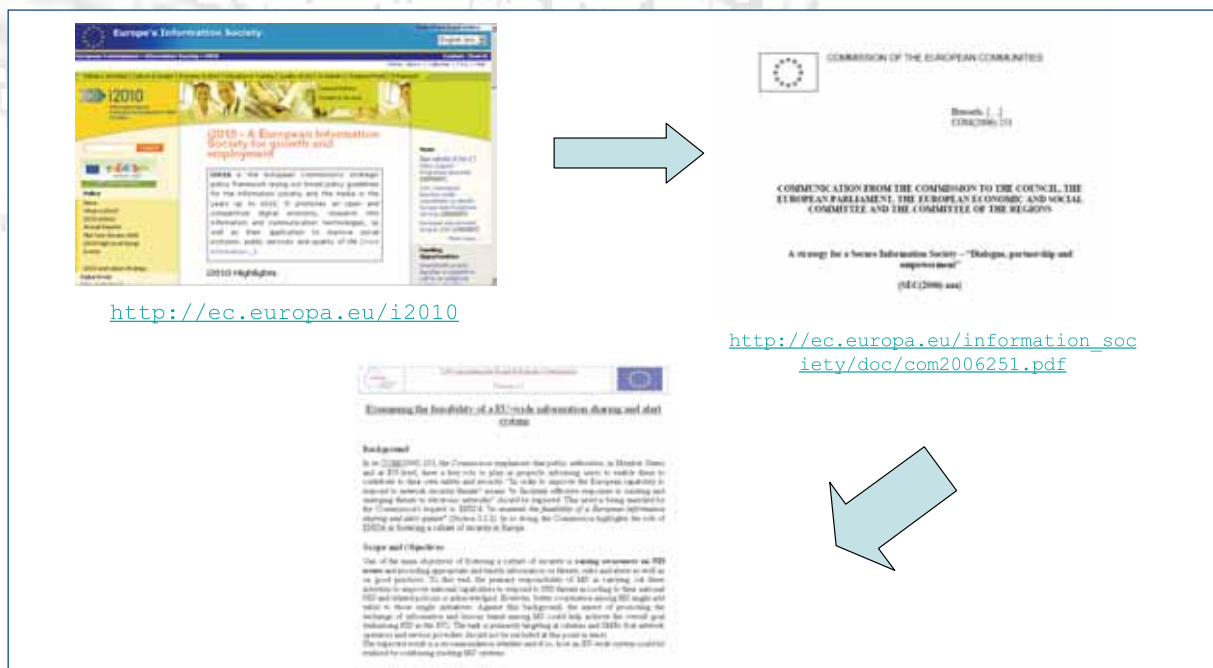


2 Context of this Study

This chapter describes the process and activities behind the request to ENISA to carry out this feasibility study. It also provides an overview of the basic parameters of the study.

2.1 A Short History of the Request to ENISA

In its communication to the Council, Parliament, the Economic and Social Committee and the Committee of the Regions (COM(2006) 251), the European Commission emphasised that public authorities in Member States and at EU-level have a key role to play in keeping home-users properly informed so that they can contribute to their own safety and security. The Commission also recognised that the possibility of facilitating “effective responses to existing and emerging threats to electronic networks” should be explored. Acknowledgement of these needs prompted the Commission’s request to ENISA to “examine the feasibility of a European information sharing and alert system (EISAS)”, highlighting the role of ENISA in fostering a culture of network and information security in Europe. ENISA accepted this request and embarked on this study.



The formal background of the feasibility study^{1, 2}

2.2 About ENISA

ENISA – the European Network and Information Security Agency – was established on 10 March 2004 for the purpose of ensuring a high and effective level of Network and Information Security (NIS) within the European Community and to develop a culture of NIS for the benefit of citizens, enterprises, public sector organisations and other consumers within the European Union.

The Agency is charged with assisting the Commission and the Member States. It co-operates with the business community, in order to help businesses meet NIS requirements, including those set out in present and future Community legislation, such as in Directive 2002/21/EC. In this way, the Agency helps ensure the smooth functioning of the Internal Market.

The Agency acts as a Centre of Excellence for the EU Member States and EU Institutions for NIS, giving expert advice and recommendations; it serves as a ‘switchboard’ for information about good practices, facilitating contacts between EU institutions, Member States and the private business and industry sectors.

Among other tasks, the Agency assists the Commission, when called upon, in the technical, preparatory work for updating and developing Community legislation in the field of NIS.

¹ i2010 – A European Information Society for growth and employment – <http://ec.europa.eu/i2010>

² COM (251)2006 – http://ec.europa.eu/information_society/doc/com2006251.pdf

3 Formal Prerequisites (Terms of Reference)

The Terms of Reference (ToR) for the feasibility study into an EISAS were agreed between the European Commission and ENISA. The complete text can be found in Annex A.

3.1 Scope and Objectives

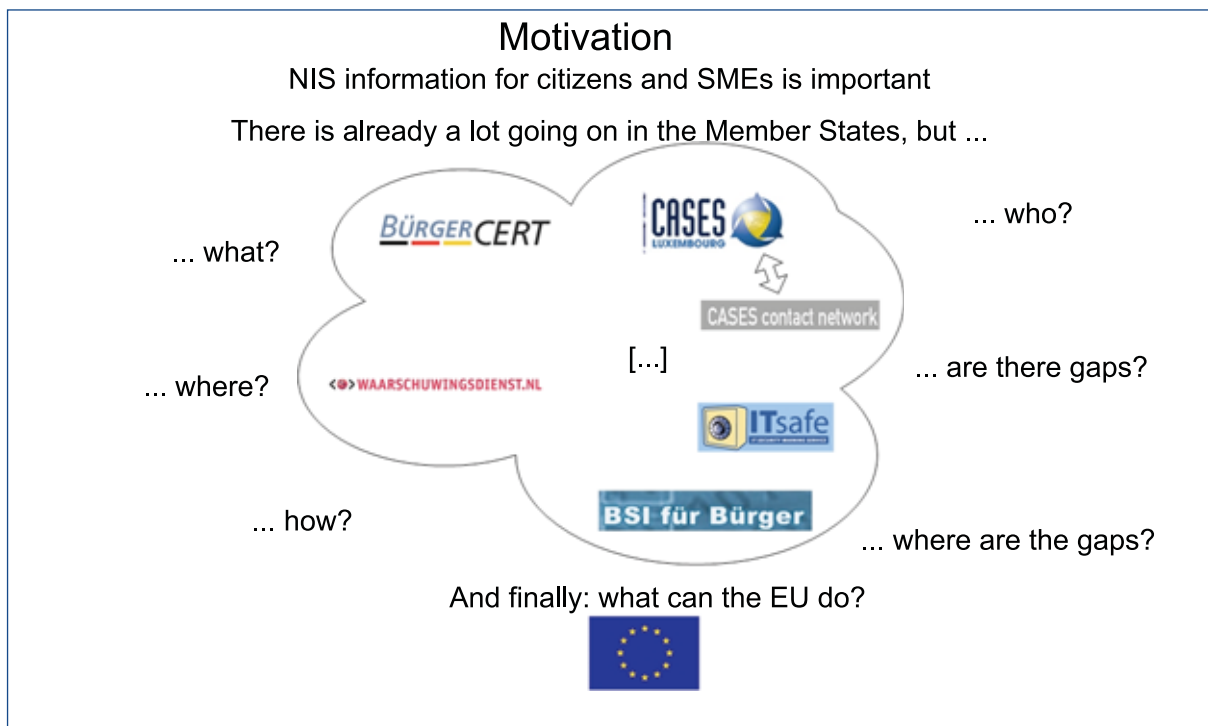
According to the ToR, the main goal of an EISAS would be to raise awareness about NIS issues among home-users and SMEs. Therefore, the expected result of the Commission's request is a recommendation whether and, if so, how, an EU-wide system could be realised in close collaboration with existing activities in the Member States. Another objective laid down in the ToR is to assess the added value of enhancing co-operation among existing activities and the added value which would be achieved for these activities as a result.

3.2 Motivation – Why Home-users and SMEs?

The communication COM (251)2006³, which is the umbrella of this feasibility study, states that “individual users need to understand that their home systems are critical for the overall ‘security chain’”. Consequently, the target audiences for a potential EISAS are home-users and Small and Medium Enterprises (SMEs).

Several publications point out that, for various reasons, the computers of home-users and SMEs are the most popular victims of targeted attacks^{4, 5}. It is comparatively easy to incorporate these users' computers into botnets, use them as obfuscated paths for launching attacks by hackers, as proxies to send spam, or to enrol them as repositories for spreading viruses and worms.

At the same time, SMEs are important to Europe's economic growth. However, due to their size, SMEs rarely employ dedicated security personnel so the protection of their information assets is often left to non-security experts.



Motivation for the feasibility study

³ COM (251)2006 – http://ec.europa.eu/information_society/doc/com2006251.pdf

⁴ OECD broadband statistics – www.oecd.org/document/7/0,3343,en_2649_34223_38446855_1_1_1_1,00.html

⁵ Symantec Memorandum to UK House of Lords – www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7013102.htm

3 Formal Prerequisites (Terms of Reference)

Taking all the above into account, this study examines the feasibility of an information sharing system for 'NIS information' (see 5.3 for a definition of this term) that:

- should primarily target individual users and SMEs
- should aim to close the gaps in the supply of these target groups with 'NIS information'
- ideally, should build upon existing information sharing activities in the Member States.

3.3 Methodology of the Feasibility Study

A set of activities was specified in the ToR in order to fulfil the Commission's request.

- **Phase I:** Analysis of the current state of affairs (chapter 6)
- **Phase II:** Examination of the feasibility of an EISAS, including a multilingual EU portal (chapter 7)
- **Phase III:** Assessment of the added value (chapter 8)
- **Follow-up:** Recommendations for next steps to be taken, based on the findings of the study (chapter 9)

3.4 Timeline of the Study

Following the schedule laid down by the ToR, ENISA started the feasibility study in October 2006. In April 2007 a joint workshop of ENISA staff, members of the Expert Group and other representatives of the Member States was held. During this meeting the findings and the approach taken to carry out this study were validated. The draft final results of the feasibility study were discussed at the IT Security Conference organised by the German EU Presidency in Berlin, on 4 and 5 of June 2007. The final report, taking into account the comments and suggestions of the Expert Group, the European Commission and the audience at the conference in Berlin, had to be finalised in November 2007.

In the meantime, several presentations were made to various audiences about the findings of the study. Without anticipating any future action by the European Commission, these presentations aimed to clarify the objectives of the Feasibility Study, and its results. A sample set of slides of one of these presentations can be found in Annex F.

A detailed timeline of this study conducted by ENISA can be found in Annex E.



4 Preparation of the Study – Setting the Scene

This chapter describes the materials and other sources that were used to prepare the feasibility study, to define starting points (initial assumptions) and cornerstones. A very brief description of the expertise of the ENISA experts in charge of this study was included, followed by essential statements and findings from projects and activities with a comparable scope which had been carried out in the past.

In particular, in addition to the two inventories specified by the ToR, the following documents were reviewed:

- The final report from the EWIS project (**European Warning & Information System**) (2001, 2002, see 4.2 below)
- ENISA's study '**CERT co-operation and its further facilitation by relevant stakeholders**' (2006, see 4.3)
- ENISA's '**Inventory of CERT activities in Europe**' (Version 06/2006 and 10/2007, see 4.4)
- The **gap analysis** produced by the ENISA Ad hoc Working Group CERT co-operation and support (2005, see 4.5)

4.1 Available Expertise in ENISA

The ENISA experts charged with carrying out the feasibility study have worked in CERTs for several years and are also involved in information sharing activities for various stakeholders. They are familiar with the different CERT communities both in Europe and beyond, and ran the two ENISA Ad hoc Working Groups on CERTs in 2005 and 2006. This expertise enabled them to accurately plan and carry out this study. The assumptions made in chapter 5, which are derived from the materials available from the previous projects and activities, are consistent with the experience gained by the ENISA experts during their professional lives. In addition, the experts working on this study are both members of FIRST, the Forum of Incident Response and Security Teams.

4.2 EWIS

Important sources of 'lessons learned' were the proceedings of the EWIS activity launched by the European Commission in 2001. In two workshops in 2001 and 2002 the idea of a 'European Warning & Information System' was examined in collaboration with various stakeholders including the CSIRT community.

From the management summary:

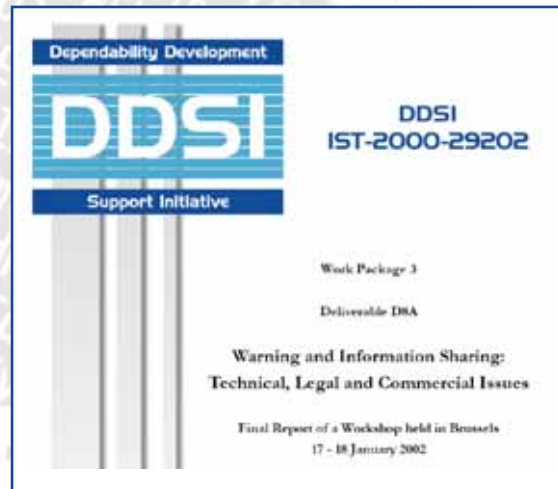
"In its June 2001 communication on network and information security the European Commission suggested a European Warning and Information System (EWIS). In October 2001 the Dependability Development Support Initiative (DDSI), the Institute for the Protection and Security of the Citizen and the Joint Research Centre organised a two-day technical workshop on EWIS [...]. The DDSI subsequently convened a two-day workshop in Brussels on 17-18 January 2002. (The) Participants were asked to reflect on the legal, commercial and architectural challenges that need to be overcome if European warning and information sharing capabilities are to be enhanced."

(Citation from the management summary of the 2nd EWIS report)



4 Preparation of the Study – Setting the Scene

Both the findings of these workshops and also the methodologies employed were helpful in planning the EISAS feasibility study, and in making some of the assumptions in chapter 4.



The EWIS report

4.2.1 Conclusions

EWIS1: A EWIS should not be a large, centralised superstructure (such a scenario was fundamentally rejected by the experts invited to the EWIS workshops). Rather it should be a small centre of facilitation, extensive (personal) networks and information dissemination channels.

Conclusion for the EISAS study: the attitude of the stakeholders did not change on this point. A newly built, centralised, co-ordinating body with operative tasks is less likely to be accepted by the relevant stakeholders than other approaches. In addition, the study must abide by its ToR which recognise:

[...] the primary responsibility of MS in carrying out these activities to improve national capabilities to respond to NIS threats according to their national NIS and related policies.

(From the Terms of Reference of the EISAS feasibility study)

EWIS2: Different target audiences have different needs as to the way information is conveyed. End-users especially must be addressed in a way that enables them to easily digest given information and (re)act accordingly. Addressing users in their native language was considered crucial. The media was suggested as a potential multiplier of NIS information to home-users and SMEs.

Conclusion for the EISAS study: this finding would be considered; indeed it was anticipated in the ToR. The EISAS feasibility study should focus (primarily) on two target audiences in order to investigate the correct way to address home-users and SMEs as comprehensively as possible. In particular, the selection of appropriate distribution channels seems to be crucial, as conventional channels such as websites and mailing lists are not always sufficient to reach either the majority of home-users and SMEs or to motivate them into action. Involving the media more effectively would seem a promising undertaking.

EWIS3: The establishment of trust (especially among CERTs) is important if information is to be shared effectively between different parties.

Conclusion for the EISAS study: this should be considered, even though shared information in the framework of an EISAS (independent of the final proposed feasible scenario) and (probably also) the contributing national ISASs is of a less operative nature than had been envisaged for a EWIS.

4 Preparation of the Study – Setting the Scene

EWIS4: CERTs/CSIRTs are predominantly involved in both reactive services (incident response) and proactive services (for example, the distribution of NIS good practice information and alerts & warnings). In addition, the majority of stakeholders invited for the two EWIS workshops were either from active CERTs or closely involved in CERT-work (such as the abuse teams of large ISPs). This strongly suggests that CERTs (and expertise in the CERT communities) will play a crucial role in the proposed scenario for an EISAS (independent of the proposed scenario), a factor which should be considered during the study.

Conclusion for the EISAS study: it seems that CERTs in the Member States play a crucial role in providing information sharing services as part of their service portfolio. This suggests that the expertise existing in the CERT communities could potentially contribute to both this study and any follow-up work based on its findings. The composition of the Expert Group should be reviewed to ensure adequate representation of the CERTs.

EWIS5: Overall it appears that the whole EWIS project was over-ambitious from the start. Early discussions suggested that the EWIS should serve all European Internet users, that it should process all kinds of relevant NIS information and should probably also be active in other areas such as reactive services. This, together with differing interpretations among the stakeholders as to what constitutes a 'European Warning & Information System', led to a rather blurred concept of a EWIS and its potential added value. This strongly suggests that a smaller, more concise and less ambitious goal would be more likely to lead to practical results.

Conclusion for the EISAS study: this was taken into account during the creation of the ToR, which lay down a much more concrete goal for an EISAS, with a more limited scope. The involvement of the stakeholders in the EISAS study should be carefully planned to avoid a divergence of concepts and discussions, and the timing of stakeholder involvement is crucial.



4 Preparation of the Study – Setting the Scene

4.3 ENISA Study ‘CERT Co-operation and its Further Facilitation...’

Previously in 2006 ENISA had produced a study that analysed the vast range of co-operation among CERT/CSIRTs and similar entities⁶. It was the first document of its kind, and not only tells the story of co-operation in Europe and beyond, but also summarises the lessons learned and offers recommendations to the stakeholders involved on how co-operation might be improved.

“This document is aimed at management, policy makers, teams and other stakeholders that, in one way or another, are involved in CERT co-operation. It should also provide an interesting read for everybody else who wants to learn about the rich culture of co-operation among European and international teams over the last two decades.”

(Citation from the management summary of the study)

The ENISA study into CERT co-operation



The study into CERT co-operation thus makes an excellent starting point in planning the follow-up to the EISAS feasibility study.

4.3.1 Conclusions

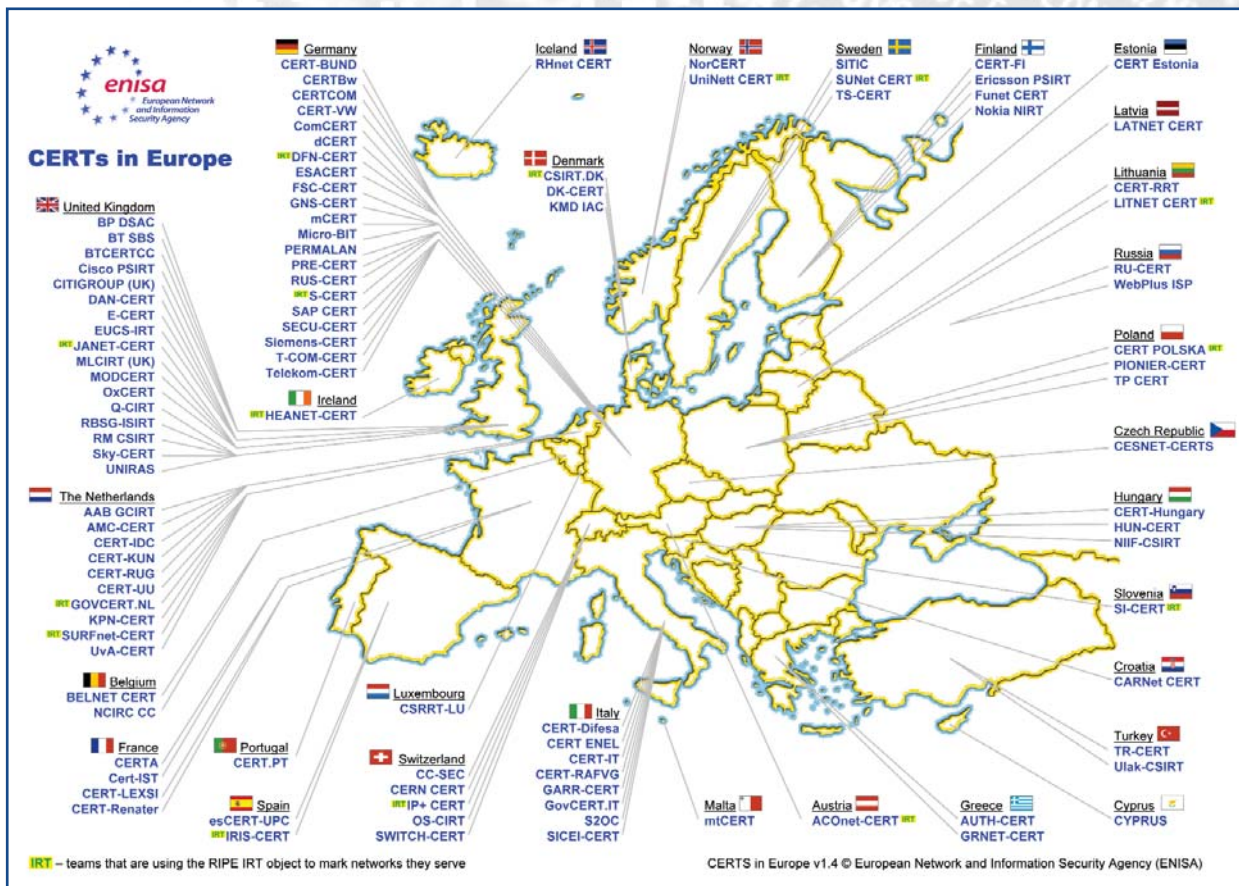
- The study provides an inventory of possible models and a legal basis for co-operation with ‘real-life examples’ that could be useful to the proposed EISAS in building on existing co-operation among national ISASs in the Member States.
- The study dedicates a section to the topic of trust-building for co-operation among different parties. This has an emphasis on CERT/CSIRT co-operation, but is also applicable to other, similarly structured groups.
- The study contains an assessment of EuroCERT which was created by the CSIRT community in the late 1990s as a Europe-wide incident response co-ordination body. EuroCERT demonstrates the problems and limitations faced by a centralised operative body in Europe. These problems, which eventually led to the failure of EuroCERT, tell us much about what is acceptable to such bodies in the field of NIS in Europe.
- The study delivers an analysis of the barriers, incentives and benefits of co-operation in various fields (including information sharing) and makes proposals for future developments. Future EISAS activities (independent of the proposed scenario) might build on these findings.

⁶ ENISA CERT co-operation study – www.enisa.europa.eu/cert_cooperation/index_cooperation.htm

4 Preparation of the Study – Setting the Scene

4.4 ENISA Inventory of CERT Activities in Europe

The Inventory⁷ lists all relevant co-operation activities in Europe and beyond that could be important to the proposed EISAS scenario, whatever its ultimate shape.



4.5 Gap Analysis

In preparation for ENISA's work in the field of CERTs, an ad hoc working group of nine independent CERT experts was formed in 2005, charged with analysing the areas where ENISA could add benefit. This gap analysis, together with the discussions in the group meetings, demonstrated that national and governmental CERTs especially were already involved in running national information sharing systems, some of them dedicated to informing citizens and SMEs in a specific Member State.

4.5.1 Conclusions

The following findings were deemed relevant to the EISAS feasibility study (the abbreviation WG stands for 'Working Group'):

WG1:

But for the last two years governments started to recognise the situation that end-users, especially private persons, are rather helpless in case of attacks. Therefore, some governments like the Netherlands and Germany have started activities to alert and inform this user-group about security issues. However, in most concepts there is no room for providing a full-fledged helpdesk for all kinds of requests of (private) end-users. In case of a high profile attack, for example a new worm that invades millions of systems at the same time, probably no governmental institution has enough resources to protect all of the private end-users to 100%, regardless how much effort has been made before.

(Final report Ad hoc WG 2005, page 7)

⁷ ENISA Inventory of CERT activities in Europe - www.enisa.europa.eu/cert_inventory/

4 Preparation of the Study – Setting the Scene

More and more systems are evolving in the Member States that target home-users and SMEs in particular but, in the case of a high profile attack, these systems will never be able to provide enough resources to cover their target groups with fully fledged helpdesk services.

Conclusion for the EISAS study: independent of the scenario ultimately proposed for an EISAS, a system that provides reactive IT security services for home-users and SMEs must take into account that, in the case of widespread incidents, the demand for resources from the service will grow exponentially and the system will probably collapse. This strongly suggests that the most feasible scenario derived and proposed in this study will be one with realistic goals – starting with a recognition that the provision of reactive services is probably not a wise choice. This realisation had already been taken into account when drawing up the ToR of the study, which limited the task of a potential EISAS to information sharing with individual users and SMEs.

WG2:

At least private end-users that are more technical interested and educated might be able to gain support and help from other available resources. Although CSIRTs usually are responsible for closed communities, much of their technical information like security advisories is publicly available, free of charge. And most existing CSIRTs belonging to national research networks will not refuse to give at least limited support, in case a victim calls its hotline.

(Final report Ad hoc WG 2005, page 7)

The crucial role of CERTs in the provision of both reactive and proactive services was confirmed. The valuable work they have already done should be taken into account.

Conclusion for the EISAS study: the assumption that (national and governmental) CERTs will play a role in the proposed scenario for an EISAS was reaffirmed.

WG3:

The gap analysis strengthens the assumption that a ‘one size fits all’ service concept in sharing NIS information with citizens and SMEs does not exist, that there are at least two kinds of users – experienced and inexperienced – and that these must be addressed differently.

Conclusion for the EISAS study: the assumption that, independent of the final proposed scenario for an EISAS, effectively addressing the target audience (individual users and SMEs) is of the utmost importance was reaffirmed.

WG4:

Finally, the gap analysis produced by the Working Group provided a very basic overview of activities in European countries in the area of CERT services (status 10/2005). The inventory of existing activities in the Member States compiled during the EISAS study will show that the situation has changed at least slightly, and additional information sharing systems are listed. The Member States have started to recognise the importance of NIS information sharing for their citizens.

Conclusion for the EISAS study: the creation of an EISAS with a supporting, facilitating and promoting role seems a promising concept. If the proposed scenario is carefully selected and respects the responsibility of the Member States for improving their national capabilities to respond to NIS threats as a primary directive, an EISAS might indeed add value for the Member States.

5 General Assumptions and Preconditions

This study aims to derive its conclusions from existing facts. However, the definition of some assumptions and preconditions is necessary to successfully carry out this feasibility study. It was recognised that all assumptions would have to be verified during the study.

5.1 Types of Potential Role for the European Union

In general it is assumed that two potential types of role for the European Union in the field of (NIS) information sharing and alerting (for home-users and SMEs) are conceivable: either to become operational itself (or to establish a new operational body) or to take the role of a facilitator, underpinning the operations of other bodies. In relation to the sharing of NIS information, alerting and warning, this would mean the EISAS should either run an information sharing and alert system (or outsource this operation to another body) for all the Member States, or should facilitate the operation of the existing information sharing activities in the respective Member States.

Obviously this model is too simplistic: among its shortcomings, the first solution would compete with existing activities in the Member States, while the second would not address the gaps in the coverage of NIS information for EU citizens and SMEs. As a result, without rejecting the idea of the two potential roles, it was recognised that the more complex 'information sharing and alerting' model would have to be divided into single components to allow a more granular feasibility study (see 5.2).



5.2 Basic Components of Information Sharing Systems

In order to carry out the study about the feasibility of an EISAS, a general model, consisting of three main components, was assumed and had to be verified during 'Phase I: Analysis of the current state of affairs' (see chapter 6). This model was intended to identify functional areas in which an EISAS could add value to existing information sharing activities in the Member States and address gaps in coverage with NIS information. The assumptions made in this chapter are based on various discussions in the ENISA Ad hoc Working Group 'CERT services' in 2006 and the Ad hoc Working Group 'CERT co-operation and support' in 2005 (in particular, the 'Gap analysis' deliverable was helpful in making these assumptions, see 4.5).

In general, a (national) information sharing and alert system ((N)ISAS) should aim to inform its users in a timely manner about NIS-related threats, vulnerabilities and countermeasures. An (N)ISAS should gather data (in a manual or automated manner), process it and finally disseminate it in various ways.

The three components of an (N)ISAS – and in general of the sub-processes of information sharing – are:

- **Information gathering component (IGC)**

An ISAS gathers raw or pre-processed information from many sources including security advisories from vendors or independent organisations, posts from security experts on mailing lists, sensor networks etc.

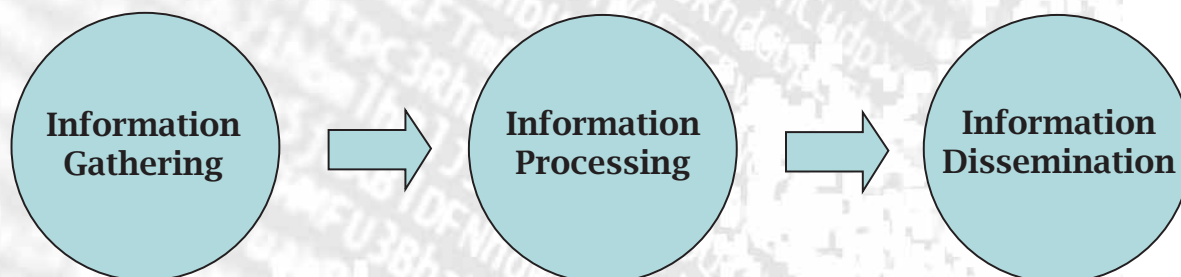
- **Information processing component (IPC)**

An important role for an ISAS is to sort and correlate the information, perhaps to weight it and to make it available for its target audiences in a suitable way (for example by tailoring the language to the needs of the target group or by rating the importance of the information).

- **Information distribution component (IDC)**

In a final step the gathered and processed information is distributed to the target audiences. Usual channels employed for this dissemination are websites or mailing lists, but perhaps also RSS-feeds, SMS notification or other suitable channels.

5 General Assumptions and Preconditions



Functional model (and sub-processes) of Information Sharing Systems

As one part of the analysis, it must be verified that, in general, the existing activities (gathered together in the first inventory, see 6.2) follow this model and that the areas where an EISAS might potentially add value (identified in chapter 8) are valid for the majority, if not all, of the existing (N)ISAS activities under consideration.

5.3 Types of Information

In order to carry out the feasibility study, the kind of information that is shared with the target audience by an ISAS was divided into three types (as proposed in the ToR). To increase the readability of this report, the proposed types of information (static information, dynamic information and real-time information) were renamed to better reflect the nature of the content.

Good NIS Practice: this self-explanatory term designates NIS information with a long-term validity that is not subject to frequent changes (for example a description of how to choose a good password, or how to identify phishing e-mails). It is assumed that this kind of information is valid (to some extent) for all home-users and SMEs in all Member States. It is the easiest kind of information that could be shared with this target audience and, after slight modifications (for example, translation), this information would also be exchangeable between separate ISASs. 'Good NIS Practice' replaces the term '**static information**' used in the ToR.

Alerts & Warnings: this term designates NIS information about short- or middle-term threats and as such has a short- to mid-term validity. To follow up the examples from the previous category, this could, for example, be a warning about an actual phishing e-mail with a specific content, aimed at customers of a specific bank. The example also shows that this kind of information may not perhaps be valid in all cases for all kinds of users and SMEs in all Member States, so it is probably not generally as easy to share with the whole target audience. A further assumption is that Alerts & Warnings should always be 'backed up' by Good NIS Practice information, so users and SMEs know how they should react to the alert or warning. It seems (and it will be shown later), that Good NIS Practice information in general should form the basic stock of every ISAS, before Alerts & Warnings are shared. 'Alerts & Warnings' replaces the term '**dynamic information**' used in the ToR.

Real-Time Information: this term designates information of an immediate nature such as netflow data or other output from sensor networks. In an aggregated and visualised format this information is of the utmost importance for CERTs, as it provides a snapshot of the actual condition of the network. Based on the findings of the EWIS project (see 4.2), we know that real-time information is not easy, perhaps even impossible, for home-users and SMEs to digest. (An analogy would be the weather forecast on television, where meteorologists have to analyse raw meteorological data and aggregate it into a suitable format before it can be understood by ordinary viewers.) Thus an ISAS that only shares real-time information is probably not targeted at home-users and SMEs. However, some Member States run such systems and, during the survey phase, contributed information about them to the inventory of existing systems in the Member States (see 6.2). They are therefore included, but a priori marked as not suitable to reach out to home-users and SMEs.

5 General Assumptions and Preconditions

5.4 The Different Aspects of Feasibility

It was clear very early that the mere technical/organisational feasibility of any kind of potential EISAS is not the only criterion this study must examine. Eventually an EISAS (whatever its ultimate shape) must be not only a technically smooth-working mechanism that shares information, but it must also fulfil additional requirements. Among other things it must, for example, not compete with any existing information sharing activity in the Member States, and it must also be accepted by the target audience – home-users and SMEs. This fact was already reflected in the ToR and thus three different aspects of feasibility were identified for further analysis in this study:

- **Technical/organisational aspect:** the technical/organisational feasibility of an EISAS, such as components and workflows etc.
- **Political aspect:** the political feasibility of an EISAS. This aspect can be reduced to the simple question: will the Member States accept and support the proposed solution?
- **Social/Cultural aspect:** the feasibility of achieving real impact by successfully, effectively and sustainably raising NIS awareness among home-users and SMEs. As will be shown later, this aspect is the most crucial, as the target groups listed have special perceptions and needs (for example, language), beginning with the fact that, in most cases, they are non-security experts.

The feasibility of an EISAS will be examined under these three aspects, starting in the next chapter with 'Phase I: Analysis of the current state of affairs'.

5.5 Potential Candidates for an Expert Group

Assembling the group of experts to support this study was left mostly to ENISA's National Liaison Officers, who were asked to nominate suitable experts for information sharing from their respective countries. However, based on discussions with the CERT communities, especially during the work of the two Ad hoc Working Groups in 2005 and 2006, and also during events and conferences such as the annual WARP Forum in the UK and the GovCERT.nl conference in The Netherlands, it was recognised that national and/or governmental CERTs in the Member States play a key role in operating and delivering content for national NIS information sharing activities. This assumption was verified in 6.2.4, and a decision had already been taken to invite mostly CERT experts to the EWIS workshops (see 4.2).



6 Phase I: Analysis of the Current State of Affairs

The ToR outline an initial phase to lay the ground for the feasibility study and to learn about the current state of affairs. The ToR specifies two inventories to be gathered, one containing existing information sharing activities in the Member States (see 6.2) and another listing publicly available sources of NIS information (see 6.3). ENISA's CERT experts also chose to review additional material that could potentially shed light on the question of feasibility in preparation for this study (see chapter 4).

6.1 Assembling the Expert Group

The national experts were nominated after consulting with the National Liaison Officers, the members of ENISA's Permanent Stakeholders' Group and members of the European Commission. After a careful examination of candidates by ENISA experts, the group was formed in February 2007, consisting of experts on national information sharing activities in various Member States and other relevant players.

The Expert Group worked mostly remotely, using e-mail. However, in April 2007 the Group met at a workshop in Brussels to discuss progress, to evaluate the findings of ENISA's experts and to consider potential scenarios for an EISAS. The minutes of that meeting can be found in Annex D.

Overall, the members of the Expert Group had to accomplish the following tasks:

- Provide information about the information sharing activities they are responsible for (thus making the vision of an EISAS more concrete)
- Assess both inventories prepared by ENISA
- Offer consultancy in the process of studying the feasibility of an EISAS
- Advise about the methodology of the study



6 Phase I: Analysis of the Current State of Affairs

6.2 Analysis of Existing Systems in the Member States

This section describes the goals, approach and results of the analysis of existing (N)ISAS activities at a national level in the Member States, and other activities.

6.2.1 Goals

In order to examine a potential role for an EISAS it was necessary to first obtain an overview of the activities run by the Member States to provide home-users and SMEs with NIS information. Only with this overview would it be possible to address all three feasibility aspects mentioned in 5.4.

Technical/organisational aspect:

The tentative model for information sharing systems in general (described in 5.2) is intended to be used for identifying functional areas in which an EISAS might add value to the existing information sharing activities in the Member States (this also has a political dimension as described in the paragraph below). One goal of the inventory and the analysis was the validation of this model and its three components, to check its accuracy and, if necessary, adjust it. A second goal of the inventory and the analysis was to discover who is responsible for operating existing activities in the Member States, in order to identify competent members for the Expert Group, as required by the Terms of Reference. A key technical/organisational question is the source of the information that existing activities use as input. This question has been addressed by a separate inventory and analysis of publicly available information sources in 6.3.



Political aspect:

The scenario derived and proposed for an EISAS must not compete with any existing system in the Member States. Only with the overview provided by the inventory of Member States' activities can the proposed scenario be evaluated in terms of this requirement. One goal of the analysis was to learn which Member States are already active in targeting their home-users and SMEs with NIS information and which plan to do so in the future. Additional goals were to identify potential areas where an EISAS might provide added value to existing activities and which Member States might contribute to this study by nominating experts for the Expert Group, as required by the Terms of Reference.

Social/Cultural aspect:

As previously stated, special techniques may be necessary to reach home-users and SMEs effectively and sustainably with NIS information. Language issues had already been cited in the Terms of Reference, but other peculiarities in addressing this target group may already have been discovered by existing activities. The inventory and the analysis aimed to identify the key criteria for successfully targeting citizens and SMEs. An additional goal was to ascertain which activities consider which key criteria, what the activities could potentially learn from each other and whether an EISAS might add value to this dialogue (without anticipating the results of the analysis, the facilitation of dialogue between the existing systems had already been identified as a potential benefit when the study began). Another goal was to verify the statement in 5.3 about the kind of information suitable for citizens and SMEs, as it is presumed that this target group cannot easily digest Real-Time Information and could become overwhelmed with alerts & warnings.

Main goals of the inventory and the analysis of existing systems:

- To discover which Member States are active in addressing home-users and SMEs, and which operate these activities, in order to assemble the most effective and competent Expert Group
- To verify or falsify the functional model of ISASs in general
- To identify the key criteria for successfully and effectively targeting home-users and SMEs, including the types of information shared

6 Phase I: Analysis of the Current State of Affairs

These main goals are subdivided into questions which the inventory and analysis of existing activities in the Member States should answer. These questions are described further in the section below. Each question is tagged according to the aspect to which it refers.

6.2.2 Questions to be answered

Key: P = political aspect, T = technical/organisational aspect, S = social aspect

Q1: What activities exist in the Member States that explicitly target citizens and SMEs? (P)

The answer to this question in particular should provide an indication as to which Member States could potentially contribute to an EISAS, and with which activities an EISAS might potentially compete.

Q2: Who operates these systems and might potentially send experts to the Expert Group to contribute to further discussions? (P/T)

There are strong indications that national/governmental CERTs play a crucial role in running this kind of information sharing service in their Member States. A positive finding here would make this study and assembling the Expert Group much easier, firstly because (to some extent) the governmental/national CERTs are already interconnected via the various CERT communities (TF-CSIRT, FIRST etc.) and secondly the ENISA experts conducting this study are very familiar with these communities and are already known to the actors.

Q3: Do the existing activities follow the three-component-model? (T)

Verification of the assumed model (see 5.2) would enable a more granular assessment of a potential role of an EISAS by analysing the potential added value in the different operational components.

Q4: What type of information is shared among citizens and SMEs? (S)

The answer to this question should indicate what the Member States consider to be valuable information for their citizens and SMEs. It should also show how information should be prepared in order to effectively reach citizens and SMEs with NIS information.

Q5: How is the information distributed? (T/S)

The answer to this question should demonstrate how Member States try to reach their citizens and SMEs. There are strong indications that a minimal set of communication channels (websites and mailing lists) is necessary for any ISAS, but that these conventional channels are probably insufficient to reach out to the majority of citizens and SMEs.

Q6: What language is used? (S)

The answer to this question should provide proof of the assumption (indicated in the ToR) that it is best to address citizens and SMEs in their native tongue.

Q7: What funding model is used? (P)

The answer to this question should indicate in general terms whether an existing (N)ISAS activity might share its information easily with a potential EISAS, or if its target groups pay for the services of the (N)ISAS, and a potential contribution of information to an EISAS would therefore need deeper analysis.

Q8: Are there interfaces to export data which might be shared with other ISASs? (T)

The answer to this question should indicate whether existing ISASs could easily share information with a potential EISAS from a technical/organisational point of view, i.e. are there already agreed data formats and mechanisms in place to export information in a sharable way, such as XML?

6 Phase I: Analysis of the Current State of Affairs

6.2.3 Methodology

The information needed to compile the inventory of existing information sharing activities in the Member States in order to analyse the current state of affairs was gathered through three different channels:

- **Expertise from various stakeholders**

ENISA used its two main channels to the stakeholders in the Member States and in other stakeholder groups. First, a questionnaire was sent to ENISA's network of **National Liaison Officers (NLOs)** with a request to submit facts about national NIS information sharing activities that primarily target citizens and SMEs. The results were compiled into the inventory of existing activities. In addition, the NLOs were asked to nominate a national expert experienced in information sharing, with a special emphasis on national activities aimed at citizens and SMEs.

- Another questionnaire was sent to ENISA's **Permanent Stakeholders' Group (PSG)**, which is the main network for relations with major stakeholders in industry, academia and consumers. Their results were also integrated into the inventory of existing information sharing activities. Section 6.1 contains more information about the Expert Group.

- **Own research and expertise**

On the advice of the CERT communities and especially the members of the Ad hoc Working Group 'CERT services' from 2006, ENISA's experts conducted their own research on the Internet about existing information sharing activities. These additional results were also incorporated into the inventory. ENISA's Inventory of CERT activities in Europe (version 1.4, December 2006) also offered additional information about national information sharing activities in the EU Member States.

The complete inventory of existing information sharing and alert systems can be found in Annex B. This information was used to answer the questions listed above in order to analyse the current state of affairs.

Disclaimer

It should be noted that the inventory was created solely for the purpose of analysing the status quo as part of this study. The information contained in this inventory was contributed either by the Member States' National Liaison Officers, the members of the Permanent Stakeholders' Group or experts in CERTs and information sharing. The inventory was as comprehensive as possible at the time of creation and during this study, but may not accurately reflect the status quo thereafter.

6.2.4 The analysis – status quo and conclusions

This section describes the analysis of the first inventory in response to the eight questions listed in 6.2.2. It should be noted that not all of the systems and activities mentioned in the questionnaire were taken into account in the analysis. A system or activity has only been mentioned here if it includes citizens and SMEs among its target groups.

Q1: What activities exist in the Member States?


For a detailed list please refer to the full inventory in Annex B.

The following table shows the known systems that share NIS information with citizens and SMEs. The specification of target groups was made by the respondents to the questionnaire, usually the NLOs of the respective Member State.



6 Phase I: Analysis of the Current State of Affairs

KEY:

 Systems dedicated to the supply of citizens and SMEs

 Systems that either count citizens and SMEs among their target groups or that plan to cover citizens and SMEs in the future

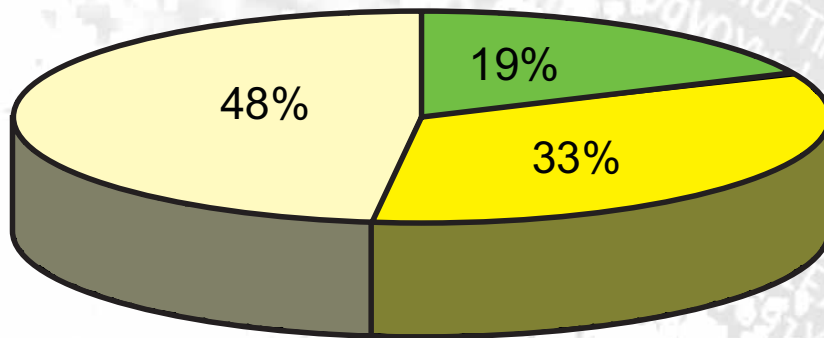
System Name	Location (Member State)	Target group
BSI fuer Buerger	GE	citizens, SMEs
Buerger CERT	GE	citizens, SMEs
CASES.lu	LU	citizens, SMEs
CERT-EE	EE	CIIP focussed (end-users planned)
CERT-FI	FI	Finnish public
CERT-PT	PT	Portuguese public
COSSI	FR	Public administration (citizens, SMEs planned)
CyTRAP Labs - CASEScontact.org	None/CH	home-users, SMEs, media
DK-CERT Vulnerability Database	DK	Danish public
Esaugumas	LT	Lithuanian public
GetSafeonLine	UK	citizens, SMEs
IT Safe	UK	citizens, SMEs
Deutschland sicher im Netz	GE	citizens, SMEs
NORCERT	NO	mainly CIIP focussed
NORSIS	NO	Norwegian public
Proventia	LV	gov.lv, municipalities
Security AR portal	EE	citizens, SMEs
Sitic - Swedish IT Incident Centre	SE	Swedish public authorities, councils, municipalities, companies
Waarschuwingsdienst	NL	SMEs, citizens

Existing (N)ISASs in the Member States

(Note: the CASES from CyTRAP Labs project is physically in Switzerland, but does provide information for a broader audience, especially Luxembourg).

6 Phase I: Analysis of the Current State of Affairs

Result: The analysis shows that 48% of the Member States (13) do not have any known ISAS activity. It also shows that 52% of the Member States (14) provide at least some information to their citizens and SMEs.



■ MS with dedicated ISAS ■ MS with non-dedicated ISAS ■ MS without ISAS

Existing (N)ISASs in the Member States

Conclusion:

- Irrespective of other information sharing activities such as CyTRAPs, there are still gaps in the coverage of the Member States regarding ISAS activities for home-users and SMEs. An EU approach should address these deficiencies.
- An EU approach should also take into account existing (N)ISAS activities and not compete with any national initiative in the Member States.



6 Phase I: Analysis of the Current State of Affairs

Q2: Who operates these systems and might potentially send experts to the Expert Group to contribute to further discussions?

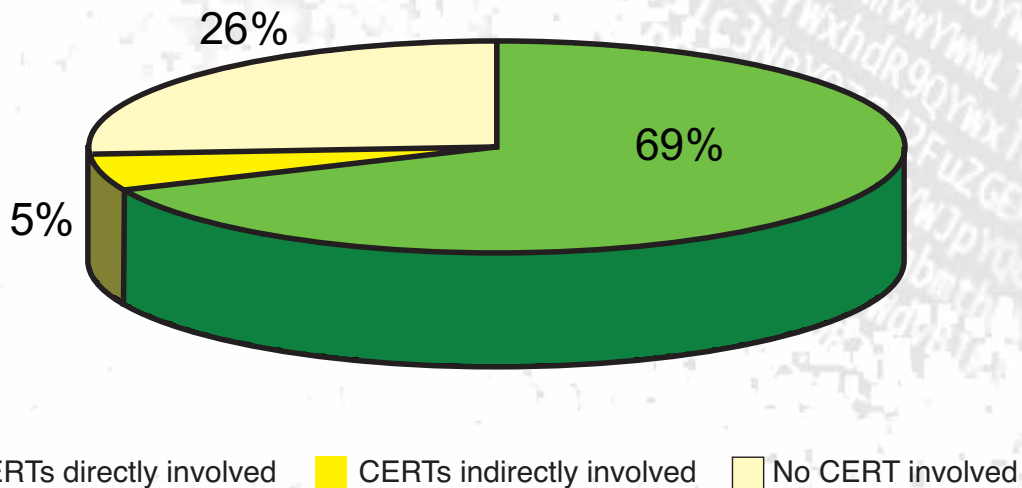
The table below summarises whether national/governmental CERTs/CSIRTs are operating an ISAS (direct involvement) or are involved as a provider of input information (indirect involvement).

System Name	Location (Member State)	CERT involved
BSI fuer Buerger	GE	Indirectly
Buerger CERT	GE	Directly
CASES.lu	LU	No GovCERT exists at the moment
CERT-EE	EE	Directly
CERT-FI	FI	Directly
CERT-PT	PT	Directly
COSSI	FR	Directly
CyTRAP Labs - CASEScontact.org	EU	Not a national initiative
DK-CERT Vulnerability Database	DK	Directly
Esaugumas	LT	Directly
GetSafeonLine	UK	Directly
IT Safe	UK	Directly
Deutschland sicher im Netz	GE	
NORCERT	NO	Directly
NORSIS	NO	
Proventia	LV	
Security AR portal	EE	
Sitic - Swedish IT Incident Centre	SE	Directly
Waarschuwingsdienst	NL	Directly

CERT involvement in (N)ISAS activities

6 Phase I: Analysis of the Current State of Affairs

Result: in the majority of cases (74%), a CERT is involved in providing ISAS services in the Member States. As the analysis of question 7 (Q7) shows (below), these are mainly national/governmental CERTs. This confirms the assumption that CERTs play a crucial role in proactive services such as NIS information sharing, and that their expertise should be taken into account in deriving the most feasible scenario for an EISAS.



CERT involvement in (N)ISAS activities

Conclusion:

- The composition of the Expert Group must be scrutinised to ensure adequate CERT representation.

Q3: Do the existing activities follow the three-component model?

Result: Without being specific, the assumption that ISASs usually follow the proposed three-component model (see 5.2) can be verified. Not a single activity listed in the inventory (see Annex B) deviates significantly from the basic model. Therefore, the model can safely be used to assess potential fields and roles of activity for the European Union.

Conclusion:

- The approach to evaluating potential roles for an EISAS with regard to the three-component model is valid.



6 Phase I: Analysis of the Current State of Affairs

Q4: What type of information is shared among citizens and SMEs?

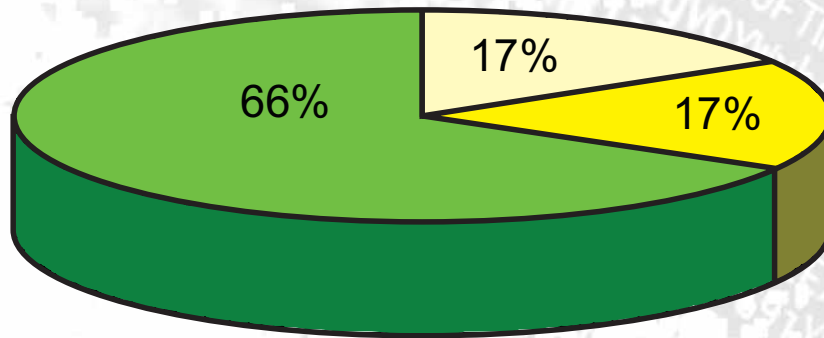
The table below lists the existing (N)ISASs and the type of information that they share with their target audiences.

System Name	Location (Member State)	Type of Information provided
BSI fuer Buerger	GE	Good NIS practice
Buerger CERT	GE	Alerts & Warnings
CASES.lu	LU	Good NIS practice, Alerts & Warnings
CERT-EE	EE	Good NIS practice, Alerts & Warnings, Real-Time
CERT-FI	FI	Good NIS practice, Alerts & Warnings
CERT-PT	PT	Good NIS practice, Alerts & Warnings
COSSI	FR	Good NIS practice, Alerts & Warnings, Real-Time
CyTRAP Labs - CASEScontact.org	EU	Good NIS practice, Alerts & Warnings
DK-CERT Vulnerability Database	DK	Good NIS practice, Alerts & Warnings
Esaugumas	LT	Alerts & Warnings
GetSafeonLine	UK	Good NIS practice
IT Safe	UK	Alerts & Warnings
Deutschland sicher im Netz	GE	Good NIS practice
MELANI	CH	Good NIS practice, Alerts & Warnings, Real-Time
NORCERT	NO	Real-Time
NORSIS	NO	Good NIS practice, Alerts & Warnings
Proventia	LV	Real-Time
Security AR portal	EE	Good NIS practice, Alerts & Warnings
Sitic - Swedish IT Incident Centre	SE	Good NIS practice, Alerts & Warnings, Real-Time
Waarschuwingsdienst	NL	Good NIS practice, Alerts & Warnings

Type of information shared

6 Phase I: Analysis of the Current State of Affairs

Result: All of the existing (N)ISASs dedicated to information sharing with citizens and SMEs share at least Good NIS Practice information. A few also include Alerts & Warnings. Special cases are Germany and the UK where different systems for each type of information exist.



■ ISAS with Good Practice ■ ISAS with Alerts & Warnings ■ ISAS with Both Types

Type of information shared

This confirms the assumption that sharing of NIS best practices constitutes a basic set of good common practice that is complemented by Alerts & Warnings in the majority of (N)ISAS activities. The two systems that only share Real-Time information do not primarily target citizens and SMEs, but in general count these as part of their target audience. Therefore, irrespective of these exceptions, the thesis that Real-Time information is considered unsuitable for this target group is supported. Furthermore, the workshop with the Expert Group found that Alerts & Warnings should always be based on good practice so that they can offer the recipient guidance on how to react to a threat. Alerts & Warnings should not fall out of the frame of Good Practice and, for new kinds of threats, the available Good Practice should be updated. In general, these findings raised even more questions about how to address the target group of citizens and SMEs effectively, and discussions during the meeting of the Expert Group resulted in a number of statements about this topic. The proposal of an EU solution should take this into account. This also probably helps answer the question as how to effectively address this target group in future steps.

Conclusion:

- It seems to be good practice to share Good Practice information and Alerts & Warnings with citizens and SMEs
- The very reasonable assumption that Real-Time information is probably not suitable for citizens and SMEs was confirmed
- Finding an adequate way to reach out to citizens and SMEs (not only with regard to the type of information that is shared) is crucial for the success of an ISAS for these target groups. Any proposed EU solution should take this into account.

6 Phase I: Analysis of the Current State of Affairs

Q5: How is the information distributed?

The table below depicts the communication channels that are used by the national ISASs to distribute their information to the target groups.

System Name	Location (Member State)	Distribution Channels
BSI fuer Buerger	GE	www, e-mail
Buerger CERT	GE	www, e-mail
CASES.lu	LU	www
CERT-EE	EE	www, e-mail, SMS, IM, RSS
CERT-FI	FI	www, e-mail
CERT-PT	PT	www, e-mail
COSSI	FR	www, mailing list, fax, mail, phone
CyTRAP Labs - CASEScontact.org	EU	www, e-mail lists, RSS
DK-CERT Vulnerability Database	DK	www, e-mail
Esaugumas	LT	www, e-mail
GetSafeonLine	UK	www, e-mail
IT Safe	UK	www, e-mail, RSS
Deutschland sicher im Netz	GE	www, e-mail
NORCERT	NO	www, e-mail
NORSIS	NO	www
Proventia	LV	www, e-mail
Security AR portal	EE	www, campaigns
Sitic - Swedish IT Incident Centre	SE	www, e-mail
Waarschuwingsdienst	NL	e-mail lists, www, SMS, media, press

Distribution channels

Results: all of the national ISASs, including those not directly targeting citizens and SMEs, at least operate a website and a mailing list. There are some activities that use additional communication channels. This suggests that the experiences of some (N)ISASs with these additional (probably not obvious) channels might be beneficial for others. In particular, the traditional media such as television, radio and the press might help to convey NIS information effectively to the end-user.

6 Phase I: Analysis of the Current State of Affairs

Conclusion:

Finding an adequate way to reach out to citizens and SMEs is crucial for the success of an ISAS for these target groups. Any proposed EU solution should take this into account. The findings of activities that have experience in addressing end-users should be considered in future steps to avoid the duplication of work.

Q6: What language is used?

The table below lists the languages in which information is shared with citizens and SMEs by the national ISASs.

KEY:



Systems that provide information in the respective native language

System Name	Location (Member State)	Language
BSI fuer Buerger	GE	German
Buerger CERT	GE	German
CASES.lu	LU	French
CERT-EE	EE	Estonian, English
CERT-FI	FI	Finish, English
CERT-PT	PT	Portuguese, English
COSSI	FR	French
CyTRAP Labs - CASEScontact.org	EU	English, German
DK-CERT Vulnerability Database	DK	Danish
Esaugumas	LT	Lithuanian
GetSafeonLine	UK	English
IT Safe	UK	English
Deutschland sicher im Netz	GE	German
NORCERT	NO	Norwegian
NORSIS	NO	Norwegian
Proventia	LV	English
Security AR portal	EE	Estonian
Sitic - Swedish IT Incident Centre	SE	Swedish
Waarschuwingsdienst	NL	Dutch

Language in which information is shared

6 Phase I: Analysis of the Current State of Affairs

Results: As anticipated, the (very reasonable) assumption that citizens and SMEs should be addressed in their native language can be verified. Nevertheless, there is a strong assumption that, to really reach out to this target group effectively, other semantic principles should also be taken into account, as most citizens and SMEs are usually non-security experts and must be addressed in an easily digestible manner. This was also the finding of the workshop with the Expert Group (see 6.4).

Conclusion:

- Any proposed EU solution should take into account the fact that citizens and SMEs should be addressed primarily in their native language.
- Finding an adequate way to reach out to citizens and SMEs (not only with regard to the communication channel) is crucial for the success of an ISAS for these target groups. The proposed EU solution should take this into account.

Q7: What funding model is used?

The following table shows the funding models adopted by ISAS activities in the different Member States.

System Name	Location (Member State)	Funding model
BSI fuer Buerger	GE	public
Buerger CERT	GE	public
CASES.lu	LU	public
CERT-EE	EE	public
CERT-FI	FI	public
CERT-PT	PT	NREN
COSSI	FR	public
CyTRAP Labs - CASEScontact.org	EU	public-private partnership
DK-CERT Vulnerability Database	DK	NREN
Esaugumas	LT	public
GetSafeonLine	UK	public
IT Safe	UK	public
Deutschland sicher im Netz	GE	public-private partnership
NORCERT	NO	public
NORSIS	NO	private
Proventia	LV	public
Security AR portal	EE	public-private partnership
Sitic - Swedish IT Incident Centre	SE	public
Waarschuwingsdienst	NL	public

Funding models

6 Phase I: Analysis of the Current State of Affairs

Results: the majority of systems are run by public authorities which reconfirms the responsibility of the Member States for ISAS activities for their citizens and SMEs. The two (national) ISASs that are run by NREN (National Research Network) CERTs are interesting. In more than one Member State the NREN CERTs (such as the DFN-CERT in Germany⁸) run their service not just for their dedicated customers, but for 'everybody interested', including home-users and SMEs, without accepting any obligation to continue this in the future or particularly addressing these target groups.

Conclusion:

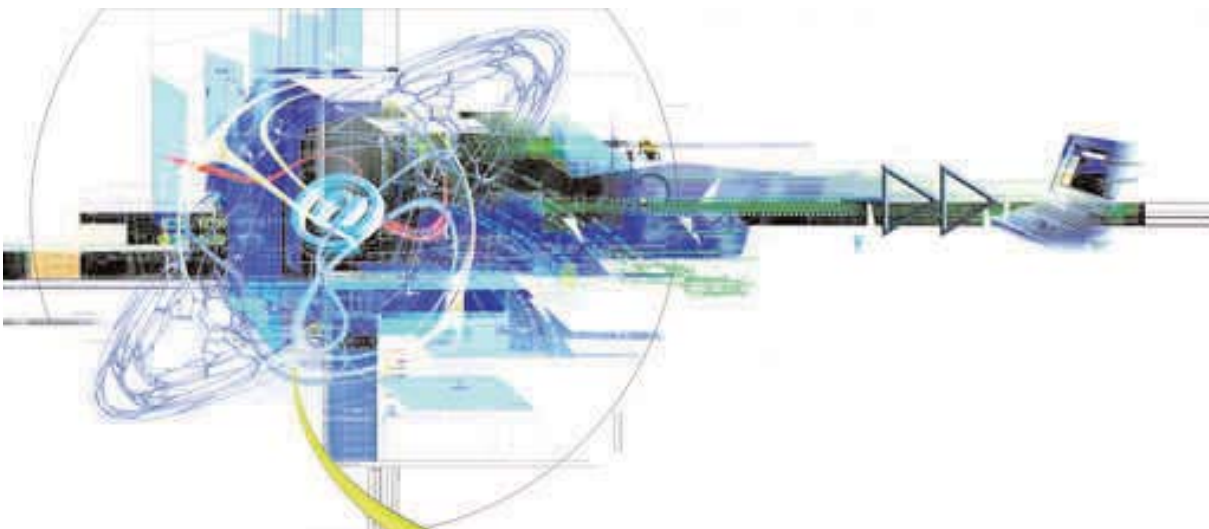
- Public funding or a public-private partnership seems to be a reasonable model to provide funding for ISAS activities.
- NREN CERTs, other sector CERTs and non-CERT activities that work in the area of sharing NIS information with home-users and SMEs (such as the various awareness-raising campaigns) are also relevant stakeholders and should be involved in potential follow-ups to this study.

Q8: Are there interfaces to export data which might be shared with other ISASs?

This question was addressed to the operators of the (N)ISAS for citizens and SMEs in the Member States at an early stage and, without being specific, it was found that almost all of the systems were considered as the end-point of information processing, implying that the information is transformed into a format suitable for direct use by the target audience. In most cases no further (automatic) sharing of the information was foreseen. Therefore, it could be concluded that the existing (N)ISASs are not prepared technically to feed their information on into other systems (including a potential EU-wide system). Some (quasi) standards for exchanging alerts, warnings and other kinds of NIS information do exist⁹ but the transformation into these formats has not yet been developed very far. This has a direct negative impact on the feasibility of a new operational information sharing body (as one of the potential scenarios for an EISAS) from a technical/organisational perspective.

Conclusion:

- Currently, almost all of the existing (national) ISAS activities are technically unprepared to share their information in an automated fashion with a potential EISAS.



⁸ DFN-CERT - www.dfn-cert.de/

⁹ For example the EISPP standard - www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

6 Phase I: Analysis of the Current State of Affairs

6.2.5 Conclusions

In summary, the analysis of the actual state of play produced the following conclusions relevant for this study:

Technical/organisational aspect

- The approach to evaluating potential roles for an EISAS with regard to the three-component model is valid.
- Public funding or a public-private partnership seems to be a reasonable model to provide funding for ISAS activities.
- Currently almost all of the existing (N)ISAS activities are technically unprepared to share their information in an automated fashion with a potential EISAS.

Political aspect

- Irrespective of other information sharing activities such as CyTRAPs, there are still gaps in the supply of NIS information for all home-users and SMEs in Europe. An EU approach should address these deficiencies.
- An EU approach should take into account existing (N)ISAS activities and not compete with any national initiative in the Member States.
- The composition of the Expert Group must be scrutinised to ensure adequate CERT (national and others) representation from the Member States.
- NREN CERTs, other sector CERTs and non-CERT activities that work in the area of sharing NIS information with home-users and SMEs (such as the various awareness-raising campaigns) are also relevant stakeholders and should be involved in potential follow-ups to this study.

Social/Cultural aspect

- It seems to be good practice to share Good Practice information and Alerts & Warnings with citizens.
- The very reasonable assumption that Real-Time information is probably not suitable for citizens and SMEs was confirmed.
- Finding an adequate way to reach out to citizens and SMEs (not only with regard to the type of information shared and the preferred communication channel) is crucial for the success of an ISAS for these target groups. Any proposed EU solution should take this into account.
- Any proposed EU solution should take into account the fact that citizens and SMEs should be addressed primarily in their native language.



6.3 Inventory of Publicly Available Sources for NIS Information

The second inventory to be compiled is an overview of publicly available sources for NIS information.

6.3.1 Goals

This inventory is intended to further evaluate potential input for an EISAS in case the proposed scenario (derived by this study) cannot build on existing (national) ISASs. As will be shown later, due to the method by which it was created (see below), this inventory might also serve as input for a good practice collection on how to successfully run a (national) ISAS for citizens and SMEs; it includes only sources that are used by CERTs (national and others) in their everyday work and thus forms an approved list of trustworthy information sources that fits perfectly into good practice collections. The proposed next steps in chapter 9 suggest other potential uses for this inventory.

6.3.2 Methodology

Existing inventories

One of the deliverables prepared by ENISA's Ad hoc Working Group 'CERT Services' in 2006 was an inventory of publicly available information sources for NIS security. The goal of this work was to provide a list of sources of information used by the participating experts in the group in their daily work, which would serve as recommendations for others, especially newly created CERTs. This comprehensive inventory formed the basis for the inventory prepared during the EISAS study and had to be modified and updated only slightly. The inventory was reused firstly to avoid duplicating work (only minor updates were necessary) and secondly because it had already been evaluated by the CERT community.

Expertise from various stakeholders

ENISA used its two main channels to the stakeholders in the Member States and in other stakeholder groups to evaluate the second inventory. The list of publicly available NIS information was sent to both NLOs and the PSG. The comments received led to only slight modifications of the original inventory prepared by the Ad hoc Working Group 'CERT services' in 2006.

Own research and expertise

Through their own research and dialogue with the CERT communities, ENISA's experts found that the inventory prepared by the Ad hoc Working Group and supplemented by the comments received through NLOs and the PSG did not need any further modification at this stage.

Disclaimer

The current inventory was produced by the ENISA Ad hoc Working Group 'CERT Services' in 2006. The information contained in that inventory was provided by the participants in this group based on their experience and may be incomplete, though it aimed to be as comprehensive as possible at the time of its creation.

6.3.3 The work

One precondition for a source of NIS-related information to be added to the inventory was its availability to Internet users in general. 'Publicly available' does not necessarily mean 'available for free', and can also include sources that are only available after subscription or paying a fee. In principle, all sources that might potentially contribute to an information sharing system (European or national) should be included here. Even if they often present similar facts, these sources (see Annex C) usually address different target groups with different levels of expertise, use different languages and different levels of detail, and have different goals such as supporting customers (vendor advisories), selling products or serving a community. Another characteristic of publicly available information is the fact that different sources provide different solutions (or mitigations for specific risk), even if the situation being covered is the same.

6 Phase I: Analysis of the Current State of Affairs

The inventory lists sources provided by different actors, including:

- **Vendors** – almost all hardware and software vendors provide information related to the security of their products. This information can usually be considered as reliable and verified, but at the same time it might be biased and dependent on the distribution policy of the source, and it might not arrive in time (for example, some security bulletins are released only once a month).
- **CERTs and independent organisations** – Many CERTs gather information from other sources such as vendors, and direct their information to a specific target audience/constituency (although it is publicly available for everyone).
- **Community sites/ mailing lists** – these are usually the sources for most recent events and the latest information. In most cases they are the first to provide information, which is often not verified.

For the complete inventory see Annex C.

The main finding based on this inventory is that many CERTs use the same sources of information to prepare the input for their contribution to (national) ISAS activities. This may lead to the conclusion that, in the area of information gathering and perhaps even processing, there is duplication of effort which may be avoidable. This finding should be assessed further, and the chapter on proposed next steps (chapter 9) will take up this issue.

An unmanageable number of potential sources and the fact that most of these are not composed in their native language adds to the confusion for inexperienced home-users or SMEs who, as a consequence, only have limited use for this 'raw information'.

6.3.4 Conclusions

- The current inventory was created by and is thus approved by CERTs active in information sharing.
- The inventory is therefore perfectly suited to be added to a good practice collection.
- The assumption that synergies between existing (national) ISAS activities can be found in the area of information gathering or even processing should be further examined.



6 Phase I: Analysis of the Current State of Affairs

6.4 The Workshop with the Expert Group

During the face-to-face meeting in Brussels the inventories and the proposed methodology for conducting the study were assessed by the group and adopted. In addition, the possible scenarios prepared by ENISA were discussed and the 'most feasible' scenario was drafted (see 7.5).

In general, during the discussions most of the assumptions and findings made so far could be confirmed. Of essential importance were the statements concerning the key elements for a successful information sharing system for citizens and SMEs that basically can be reduced to the provision of information in an adequate way to reach out to this target group effectively and, as a consequence, to initiate a change of behaviour.

6.4.1 Conclusions

The following are the main comments (taken from the minutes, see Annex D) made in the workshop:

- end-users and SMEs should be addressed in their **native language**. (EG1)
- the messages (warnings, good practice documents etc.) should be phrased semantically in an **understandable way** (i.e. addressing the non-expert). (EG2)
- the method of disseminating information should be thoroughly planned, i.e. other ways besides web pages and mailing lists should be examined including podcasts, RSS-feeds, traditional media etc. It should be made as **convenient** as possible for the end-user/SME to obtain the information. (EG3)
- **avoid** information **overflow**; thoroughly plan what to publish and when to publish it. (EG4)
- information disseminated to end-users/SMEs must be **trusted** by the recipients for it to be accepted (on average, national governments are already trusted by end-users/SMEs). (EG5)
- information should be disseminated as **close** to end-users/SMEs as possible. (EG6)
- **advertise** the system; an information sharing system will only be used when people know it exists. (EG7)

The participants also reconfirmed their lack of acceptance of a new centralised body with an operational function (EG8). Finally, the difficult determination of Key Performance Indicators (KPIs) to measure the success of ISASs in general and an EISAS in particular was discussed.

6.5 Conclusions and Starting Points for Phase II

In summary, the analysis of data gathered in previous projects and of the actual state of play provided the following key interim conclusions to this study:

6.5.1 Technical/organisational aspect

- Start small, but think big. Do not be overambitious and carefully select the scope and stakeholder involvement. (EWIS5)
- There are strong indicators that the most feasible scenario derived and proposed in this study would have realistic goals – starting with the provision of reactive services is probably not a wise choice (again 'Start small, but think big'). (WG1)
- The approach to evaluating potential roles for an EISAS with regard to the three-component model is valid. (Q3)
- Public funding or a public-private partnership seems to be a reasonable model to provide funding for ISAS activities. (Q7)
- Almost all of the existing (national) ISAS activities are currently technically unprepared to share their information in an automated fashion with a potential EISAS. (Q8)
- Establishment of trust between different parties is important if information is to be effectively shared between them. (EWIS3)
- Material prepared and maintained by ENISA is useful in facilitating the proposed next steps.

6.5.2 Political aspect

- Irrespective of other information sharing activities such as CyTRAPs, there are still gaps in the supply of NIS information for all home-users and SMEs in Europe. An EU approach should address these deficiencies. (Q1)

6 Phase I: Analysis of the Current State of Affairs

- There are gaps in the coverage of home-users and SMEs with adequate NIS information in the Member States. (WG5)
- An EU approach should also take into account existing ISAS activities and should not compete with any national initiatives in the Member States. (Q1)
- Information disseminated to end-users/SMEs must be trusted by the recipients for it to be accepted (on average, national governments are already trusted by end-users/SMEs) (EG5)
- Information should be disseminated as close to end-users/SMEs as possible. (EG6)
- Advertise the system; an information sharing system will only be used when people know it exists. (EG7)
- A newly established, centralised co-ordinating body with operative tasks is less likely to be accepted by the relevant stakeholders than other approaches. This reconfirms the statement about the responsibility of the Member States made in the ToR. (EWIS1)
- The experts in the Expert Group reconfirmed their lack of acceptance of a new centralised body with an operational function. (EG8)
- The composition of the Expert Group must be scrutinised to ensure adequate CERT (national and others) representation from the Member States. (Q2)
- NREN CERTs, other sector CERTs and non-CERT activities that work in the area of sharing NIS information with home-users and SMEs (such as the various awareness-raising campaigns) are also relevant stakeholders and should be involved in potential follow-ups to this study.
- CERTs are predominantly involved in both reactive services (incident response) and proactive services (alerts & warnings) and their expertise should be taken into account. (EWIS4)
- The assumption that (national and governmental) CERTs would play a role in the proposed scenario for an EISAS was reaffirmed. (WG2)
- Material prepared and maintained by ENISA is useful in facilitating the proposed next steps.

6.5.3 Social/Cultural aspect

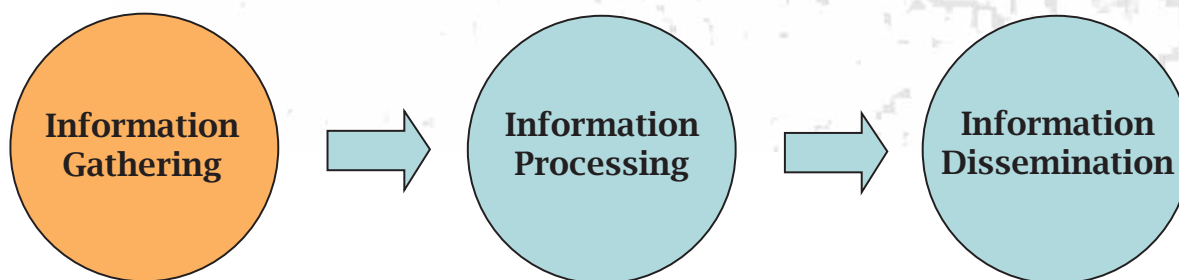
- It seems to be good practice to share Good Practice information and Alerts & Warnings with citizens. (Q4)
- The very reasonable assumption that Real-Time information is probably not suitable for citizens and SMEs was confirmed. (Q4)
- Finding an adequate way to reach out to citizens and SMEs (not just with regard to the type of information shared and the preferred communication channel) is crucial for the success of an ISAS for these target groups. Any proposed EU solution should take this into account. (Q5)
- Any proposed EU solution should take into account the fact that citizens and SMEs should be addressed primarily in their native language. (Q6)
- End-users and SMEs should be addressed in their native language. (EG1)
- Messages (warnings, good practice documents etc.) should be phrased semantically in an understandable way (i.e. they should address the non-expert). (EG2)
- The method of disseminating information should be thoroughly planned, i.e. other ways besides web pages and mailing lists should be considered, such as pod casts, RSS-feeds, traditional media etc. It should be made as convenient as possible for the end-user/SME to obtain the information. (EG3)
- Avoid information overflow; thoroughly plan what to publish and when to publish it. (EG4)
- Information disseminated to end-users/SMEs must be trusted by the recipients for it to be accepted (on average, national governments are already trusted by end-users/SMEs). (EG5)
- Information should be disseminated as close to end-users/SMEs as possible. (EG6)
- The EISAS feasibility study should focus (primarily) on two target audiences in order to investigate the correct way to address citizens and SMEs as comprehensively as possible. In particular, the selection of appropriate distribution channels seems to be crucial, as conventional channels such as websites and mailing lists are not always sufficient either to reach the majority of citizens and SMEs or to motivate them into action. Involving the media more effectively would seem a promising undertaking. (EWIS2)
- The assumption that effectively addressing the target audience (citizens and SMEs), independent of the final proposed scenario for an EISAS, is of the utmost importance was reaffirmed. (WG3)
- Advertise the system; an information sharing system will only be used when people know it exists. (EG7)
- Material prepared and maintained by ENISA is useful in facilitating the proposed next steps.

7 Phase II: Examination of the Feasibility of an EISAS

The main goal of this phase was to derive the most feasible scenario for an EU-driven activity in order to raise awareness among citizens and SMEs in the Member States from the conclusions drawn in Phase I. As explained in 5.1, the role of the EU might be either operational or facilitating. The verified model for a generic ISAS (see 5.2) will be used to identify areas in which the EU might potentially become active. Taking into account the conclusions from Phase I, the advantages and disadvantages will be assessed and the potential added value of an EU-driven activity for Phase III will be described. Finally, a description of a model of EU activity that seems to provide the greatest benefit for the existing information sharing landscape will be derived.

NOTE: In this chapter the terms 'solution', 'model' or 'role' are not used in any specific sense, and only very general statements concerning actual implementation are made. This is intentional, to avoid focusing on the specific implementation (or prototype) of a proposal in this phase; rather the implication which a specific action by the European Union would have in principle is assessed. Only the 'multilingual platform' is addressed directly, as this implementation was mentioned in the ToR.

7.1 Information Gathering



7.1.1 Potential operational roles

An operational role in the area of information gathering would mean to run (or outsource) a dedicated system for information gathering using the sources listed in the inventory of publicly available sources of security information (see 6.3). Pre-processing the information and making it available to interested parties (especially existing (N)ISASs in the Member States) or using the information in its own dedicated Information Processing System (see paragraph below) would also be included in the definition of an operational role.

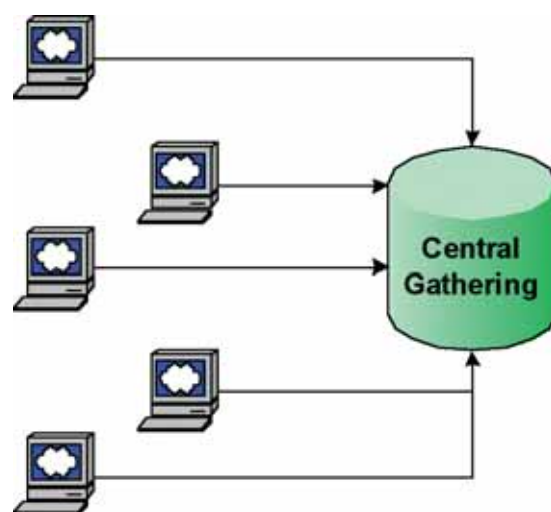
Technical/organisational aspect:

This model is feasible with a large budget and staff, using operational models from other (national) ISASs. The lack of easily exportable information from existing ISASs (see 6.2.2, Q8) would be an obstacle; information would have to be gathered the 'conventional' way, as it is by the (N)ISASs.

Political aspect:

An operational role in information gathering competes with existing activities in the Member States as information gathering and pre-processing already form part of the work of every national ISAS (however see also 'Potential added value' below).

In addition, similar factors which contributed to the failure of EuroCERT (see 4.3) would make acceptance of this model by these Member States at best questionable.



Operational role in information gathering

7 Phase II: Examination of the Feasibility of an EISAS

Cultural/social aspect:

As information is not distributed to citizens and SMEs directly, this aspect is not addressed here.

Potential added value:

For MSs with existing ISASs: if accepted by the Member States (the national ISAS activities), centralised information gathering could help to avoid the duplication of work for the existing ISASs, as pointed out in 8.4.

For MSs without ISASs: this measure alone would not add any value to these MSs, but could potentially assist them in setting up their own (N)ISAS.

7.1.2 Potential facilitating roles

Collecting and sharing good practice in information gathering, especially providing a frequently updated list of publicly available information sources, but also other practices including pre-selection of information, pre-processing etc.

Technical/organisational aspect:

Facilitation would not need any technical implementation, when existing resources could be used, but organisational co-ordination might be required.

Political aspect:

The proposed scenario would not compete with any national ISAS in the Member States. The acceptance by these Member States would be high, if they could be motivated to contribute to the good practice collection.

Cultural/social aspect:

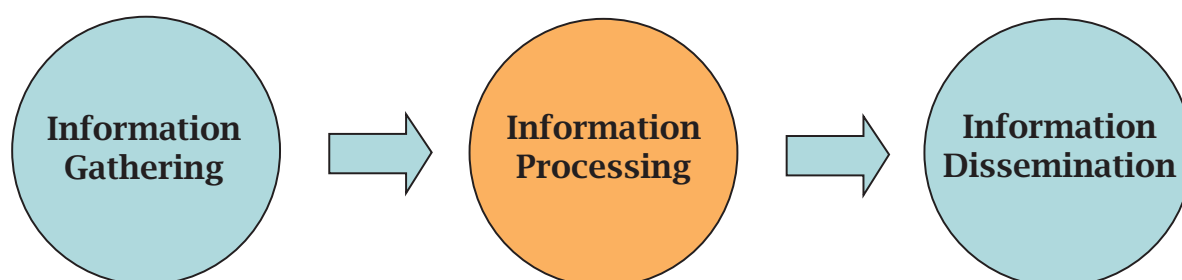
As information is not distributed to citizens and SMEs directly, this aspect is not addressed here.

Potential added value:

For MSs with existing ISASs: these Member States could contribute to the good practice collection and help with the dissemination. This would also make it possible to export 'their way' of information sharing and alerting to other MSs. On the other hand, they might also benefit by learning from other national ISASs.

For MSs without ISASs: this measure alone would not add any value to these MSs, but could potentially assist them in setting up their own national ISASs.

7.2 Information Processing



7.2.1 Potential operational roles

Processing, in this context, means to transform information into a format that can be distributed to, and using 'wording' that is understood by, the target audience. An operational role in this part of the process would mean to provide that service and distribute processed information to the existing ISASs, which would then distribute it to their target audiences. The processed information could also be used in its own (centralised) information dissemination system (see paragraph below).

7 Phase II: Examination of the Feasibility of an EISAS

Technical/organisational aspect:

This model is feasible with a large budget and staff; translation of the NIS information into other EU languages would be necessary, if this could not be undertaken on the recipient's side.

Political aspect:

This model would compete with existing activities in the Member States, as information processing is already part of the work of every national ISAS. Similar factors which contributed to the failure of EuroCERT (see 4.3) would make acceptance by the Member States unpredictable.

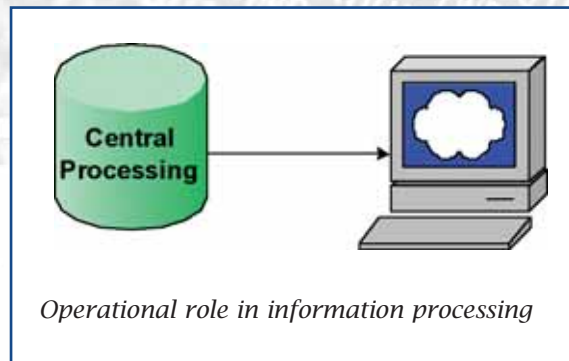
Cultural/social aspect:

Centralised processing would not take into account national or regional particularities, especially language.

Potential added value:

For MSs with existing ISASs: if accepted, central information processing could (to some extent) help to prevent the duplication of effort for the existing (N)ISASs.

For MSs without ISASs: this measure alone would not add any value to these MSs, but could potentially assist them in setting up their own (N)ISAS.



7.2.2 Potential facilitating roles

Collect and share good practice in information processing. This includes guidelines on how to formulate technical details in a way that is understood by citizens and SMEs.

Technical/organisational aspect:

Facilitation would not need any technical implementation, when existing resources could be used, but organisational co-ordination might be required.

Political aspect:

The proposed scenario would not compete with any national ISAS in the Member States. The acceptance by the Member States would be high, if they could be motivated to contribute to the good practice collection.

Cultural/social aspect:

As information is shared especially with potential new national ISASs, this solution is much better suited to take into account regional, cultural and social particularities. Otherwise this aspect is not directly addressed.

Potential added value:

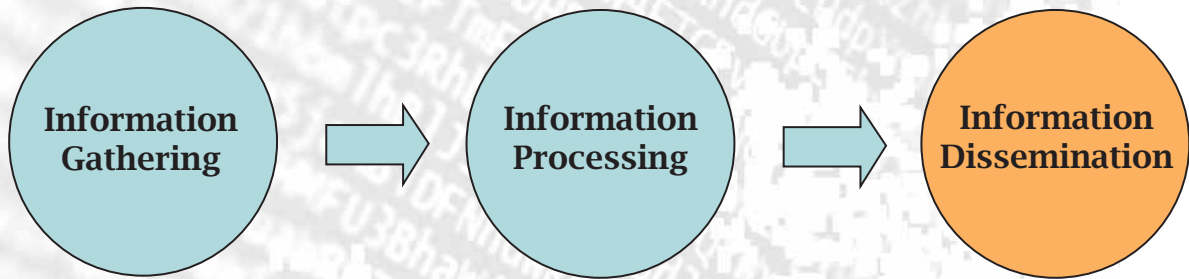
For MSs with existing ISASs: these Member States could contribute to the good practice collection and help with the dissemination. This would also make it possible to export 'their way' of information sharing and alerting to other MSs. On the other hand they could also benefit by learning from other national ISASs.

For MSs without ISASs: this measure alone would not add any value to these MSs, but could potentially assist them in setting up their own national ISASs.



7 Phase II: Examination of the Feasibility of an EISAS

7.3 Information Dissemination



7.3.1 Potential operational roles

An operative role in information dissemination would mean to operate (or to outsource) communication channels that transport NIS information directly to the citizens and SMEs in the Member States. This is also where a multi-language portal would be placed because, in order to effectively reach citizens and SMEs, all information would have to be provided in the various languages spoken in the Member States. Other communication channels are conceivable with limitations (see below 'Political aspect' and 'Cultural/social aspect').

Technical/organisational aspect:

This solution would be feasible with a very large budget and staff. All information would have to be gathered, either by the EISAS's own (centralised) information gathering facility (see above) or by making use of the input provided by existing national ISASs. In this case, either a careful selection of providing ISASs or of incoming material would have to be made in order to avoid overwhelming the target group with information. All material would have to be translated into (a subset of) the languages spoken in the Member States.

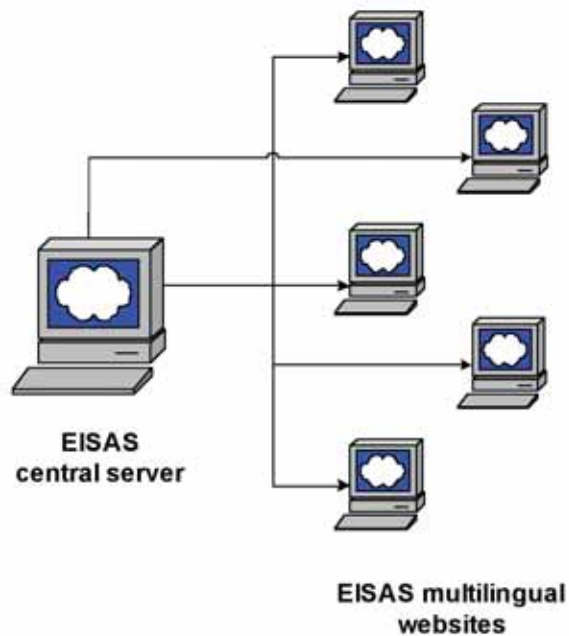
Political aspect:

This solution is the most problematic when it comes to acceptance by the Member States. If all the languages spoken in the Member States were covered, this solution would clearly compete with all the existing national ISASs. If only the languages of Member States without any national ISAS

were covered, this would exclude the Member States with an official language that is also spoken in a Member State with a national ISAS (for example Germany is a Member State with a national ISAS and Austria, whose native language is also German, is a Member State without a national ISAS). Furthermore, the implementation would have to be very flexible and stop providing NIS information in a specific language when the respective Member State sets up its own national ISAS. This solution would also need to either have its own information gathering and processing units, or the national ISASs (or other information providing services) would have to produce exchangeable NIS information to be able to disseminate to citizens and SMEs (see also 'Cultural/social aspect'). In the latter case, incentives would have to be found to encourage the support of this solution by the Member States.

Cultural/social aspect:

The information shared by this solution, even if provided in the mother tongue, could not satisfactorily take into account regional or cultural particularities for all citizens and SMEs within the European Union. To some extent the solution could effectively provide good NIS practice information, but it would fail, for example, to warn in case of a targeted phishing attack that only affects customers of a local branch of a bank. In any case, this solution would contradict the finding in Phase I that NIS information should be distributed as close to the citizens and SMEs as possible in order to be trusted enough to have an impact.



Operational role in information dissemination

7 Phase II: Examination of the Feasibility of an EISAS

Potential added value:

For MSs with existing ISASs: this solution offers no obvious added value for these Member States. Some of these MSs might be encouraged to contribute to an implementation based on this solution in order to support citizens and SMEs in other MSs, but it would not have any impact on the citizens and SMEs in their own country.

For MSs without existing ISASs: this solution, if accepted by these MSs, would be good to close the existing gap in the coverage of their citizens and SMEs on a temporary basis, but the shortcomings addressed above under 'Cultural/social aspect' would still apply.

7.3.2 Potential facilitating roles

A facilitating role in this area (as in the other areas addressed above) would be the collection and sharing of good practice in information dissemination to citizens and SMEs. This would also have to take into account all the points made in the results of Phase I, such as how to correctly address citizens and SMEs, what are the appropriate communication channels etc.

Technical/organisational aspect:

Facilitation would not need any technical implementation, when existing resources could be used, but organisational co-ordination might be required.

Political aspect:

The proposed scenario would not compete with any national ISAS in the Member States. The likelihood of acceptance by these Member States would be high, if they could be motivated to contribute to the good practice collection.

Cultural/social aspect:

The facilitation and the support for national ISASs in the Member States (by sharing good practice with them) is well suited to take into account regional, cultural and social particularities.

Potential added value:

For MSs with existing ISASs: these Member States could contribute to the good practice collection and help with dissemination. This would also make it possible to export 'their way' of information sharing and alerting to other MSs. On the other hand, they could also benefit by learning from other national ISASs.

For MSs without ISASs: this measure alone would not add any value to these MSs, but could potentially assist them in setting up their own national ISAS.



7 Phase II: Examination of the Feasibility of an EISAS

7.4 Conclusions

This section compares the pros and cons of both potential roles; the operational role and the facilitating role.

7.4.1 Operational role

As an overall assessment of the analysis recorded in this chapter, it can be concluded that an operational role in any of the functional areas of information sharing has shortcomings that are greater than those associated with a facilitating role.

The shortcomings of an operational role from a **technical/organisational** perspective could probably be solved by making available enough resources in the form of staff, funds and effort, so that the implementation of all of the proposed operative roles would become technically feasible.

With sufficient staff, funds and effort, the shortcomings from a **cultural/social** perspective could also be addressed, but would probably not be solved completely (the principle of delivering information as close to the end-user as possible would always be neglected).

The greatest problem in an operational role (in either one or all of the functional areas) lies in the **political** aspect – mainly the expected lack of acceptance by the Member States, especially those with existing national activities. In particular, a role in information dissemination contradicts the principle of the Member States having responsibility for improving their national capabilities to respond to NIS threats according to their national NIS and related policies. However, some examples of operational areas with a potential for improvement by an activity of the European Union were identified (such as in the functional area of information gathering). These should be monitored and discussed further in future steps, but an operational activity by the European Union would probably not address them effectively.

7.4.2 Facilitating roles

On the other hand, the role of a facilitator for the European Union seems much less problematic and offers much more potential than an operational role. A very promising role for the European Union lies in acting as a clearing house for good practice concerning information sharing and alerting for citizens and SMEs, as a facilitator for the dialogue between the Member States and, last but not least, in supporting Member States in setting up their own national ISAs for their citizens and SMEs.

From a **technical/organisational** perspective, this role would not need much implementation if existing facilities could be used, but organisational co-ordination might be required. Indeed there is strong evidence to suggest that ENISA could play a significant role here, as the Agency has already established the 'NIS brokerage' system which aims to support the collaboration of Member States in NIS (see 9.3).

From a **political** perspective, a facilitating role for the European Union would also be much more likely to succeed than an operational role. The main reason is that many Member States are already active in informing their home-users and SMEs about NIS issues; a Europe-wide solution would build on these activities and, ultimately, should add value to these Member States. This would be achieved by making the collected good practice also available to existing activities and fostering a dialogue between them so that they could learn from others (and optimise their own systems).

Limiting the scope of the EISAS to a facilitating role is also preferable from a **cultural/social** perspective, mainly because (N)ISAs are much better suited to take into account regional, cultural and social particularities related to their own citizens and SMEs.

Therefore, based on the findings of this study, a facilitation and good practice framework is suggested as the most feasible and most promising role for the European Union (see below).

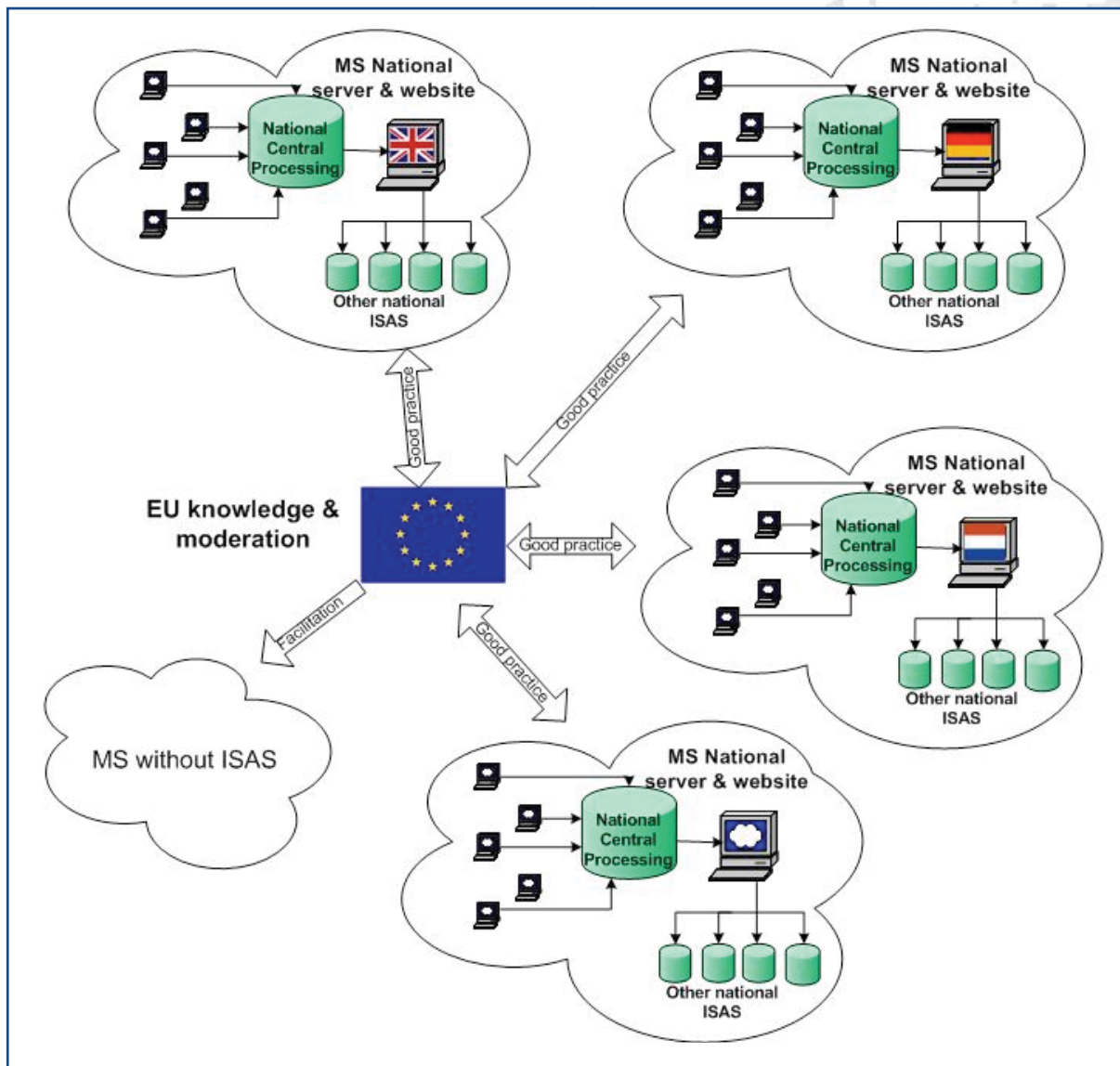
7 Phase II: Examination of the Feasibility of an EISAS

7.5 Proposed Scenario

The findings in this chapter almost unanimously suggest the greater feasibility of a facilitating role for the European Union rather than an operational role, in all of the relevant aspects. The most feasible scenario proposed consequently places the European Union at the centre of a framework for knowledge sharing, discussion fostering and the support of planned and existing national initiatives. The proposed role is three-fold:

- Act as a clearing house for good practice to support new national systems in the Member States

The European Union should use its neutral and central position to generate, administer and continuously update a collection of good practices of information sharing and alerting for citizens and SMEs. It first has to evaluate how this task might be achieved, how a basic set of good practices might be generated and what should be included. The collected good practice should then be transformed into an action plan that is easy to apply in Member States that want to set up their own (N)ISAS. The European Union should also act as a broker for contact information to all relevant players in the field that can join together in order to build a kind of 'task force' to support the Member States with their expertise. The existing national ISASs are a natural part of this group of players. The incentive for the national ISASs to contribute to this supporting framework for new ISASs ties in closely with the second role for the European Union described in the paragraph below.



Clearing house for good practice

Chapter 9 lists the recommendations for implementation of this role, together with further examples.

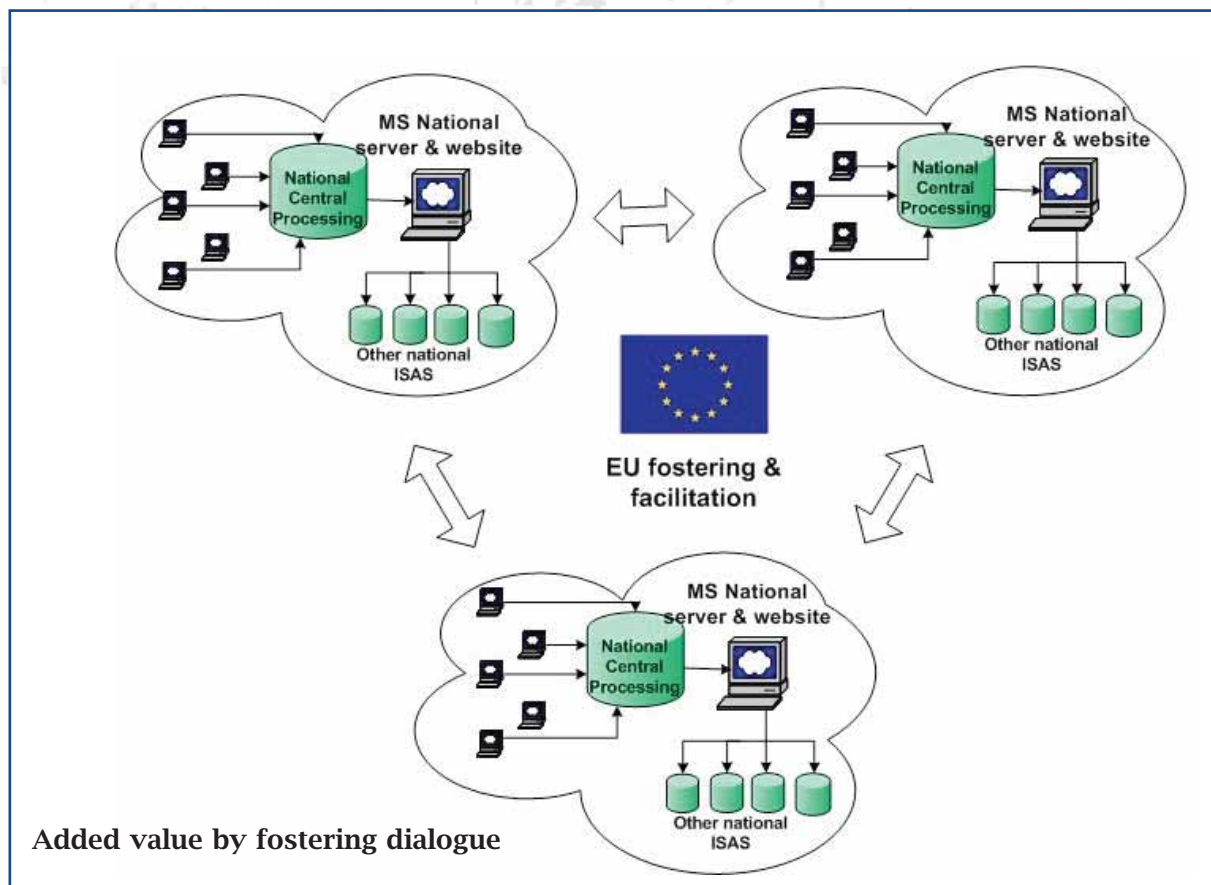
7 Phase II: Examination of the Feasibility of an EISAS

- Act as a facilitator of discussions between national ISASs in the Member States

The second role the European Union should play is that of a fosterer and facilitator of discussion among the existing national ISASs (and other appropriate activities). There are three main goals to achieve here:

- help the existing activities to learn from each other (as there is no single activity that does everything with 100% effectiveness)
- continuously update the good practice collection referred to above
- together identify areas where a common activity would help to improve the service level of all the activities

The good practice collection maintained by the European Union should act as an incentive for the existing activities to contribute to the framework, as these existing activities should also be able to benefit from it and learn from the lessons learned by other Member States. In addition, joint actions could help to improve the service level in all the existing ISASs, for example, a study on how to correctly address a specific group of citizens with what kind of information. In this dialogue the extension to reach out to new target groups besides citizens and SMEs could also be discussed and reflected in the good practice collection and the action plan(s).



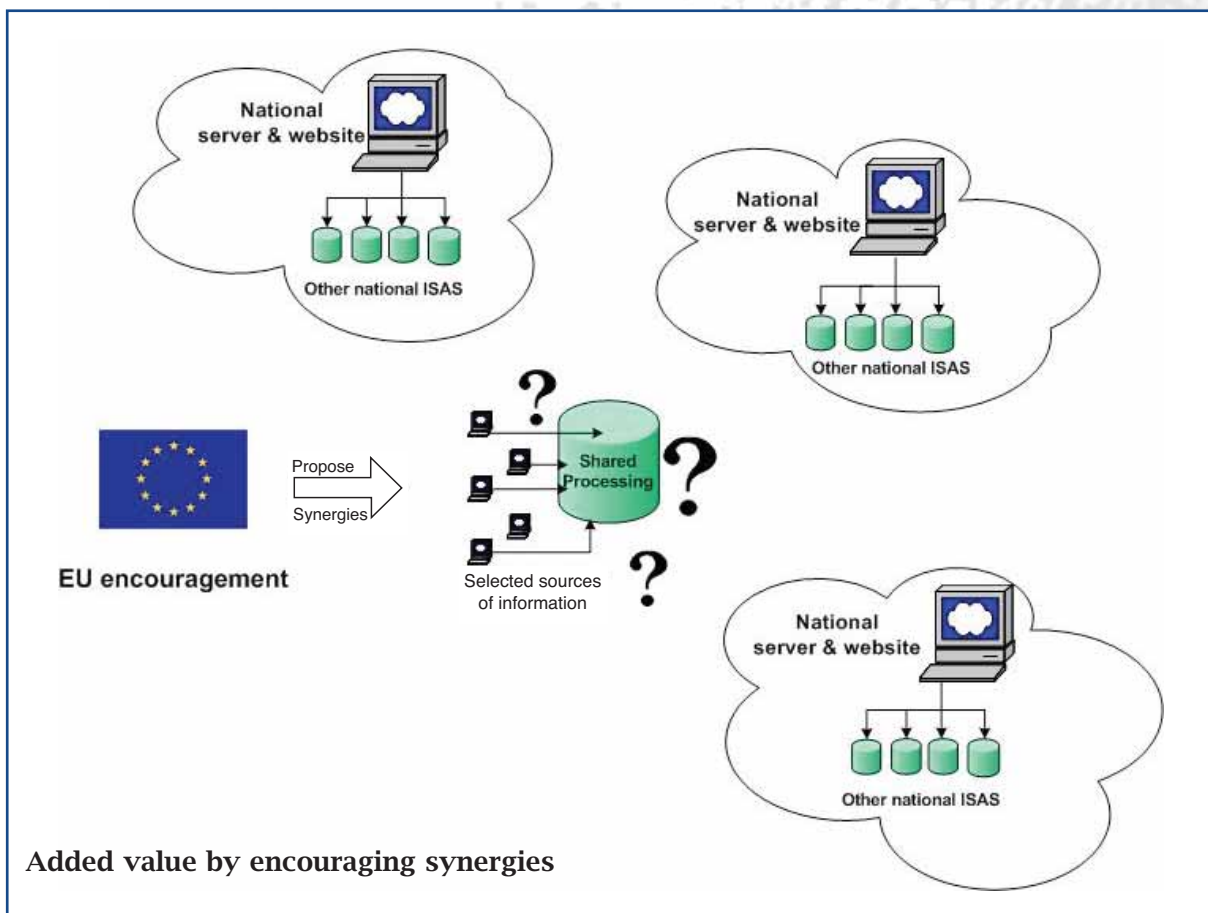
Facilitator of dialogue

Chapter 9 lists recommendations for implementation of this role, together with further examples.

7 Phase II: Examination of the Feasibility of an EISAS

- Act as an analyst of the collected good practice and, if appropriate, propose areas of optimisation

There is a potential third role for the European Union that could be adopted after the first two roles (described above) have proved their added value in practice. Once the good practice collection is reasonably comprehensive, the dialogue between the national ISASs (and other relevant players) is in progress and perhaps new national ISASs have been set up using the framework described above, a revision of the good practices, the components of information sharing and the necessary processes could be facilitated by the European Union. As a result, additional areas might be identified where new operational components could add value by centralising tasks that are necessary for all the national ISASs. The new operational components would not necessarily have to be installed (and certainly not necessarily by the European Union) but could perhaps be achieved by a rearrangement of existing components.



Analyse and propose synergies

A potentially promising first area of optimisation was discussed during the workshop with the Expert Group and will be elaborated further in chapter 9.

7.6 Starting Point for Phase III

The following four components comprise the proposed most feasible and promising scenario:

- To act as a clearing house for good practice for national ISASs
- To support new national ISASs
- To foster dialogue between existing national ISASs
- To analyse and review practice, components and processes to optimise information sharing for the existing ISASs

These components will be analysed for their added value in the next chapter.

8 Phase III: Assessment of the Added Value

The third phase of the study consists of the analysis of the added value that the attributes of the three potential roles of the European Union would bring to EU Member States which either have or do not have a national ISAS. Some of the following information has already been mentioned previously, but is repeated here in the interests of traceability and logical sequence.

8.1 Act as a Clearing House for Good Practice for National ISASs

Added value for Member States with national ISASs

- There would be an opportunity for the good practice that these Member States have already collected by running their own systems to be shared with others, without the burden of the MSs having to maintain the material themselves.
- The contributing Member States would receive acknowledgement for their achievements in the form of appreciation by the users of their contributions.

Added value for Member States without national ISASs

- The receiving Member States would receive a well maintained set of good practice that had been collected throughout Europe from a neutral source.

8.2 Support New National ISASs

Added value for Member States with national ISASs

- The Member States with existing national ISASs would gain new counterparts who would join in the discussion fostered by the European Union.
- The pool of good practice would be extended by these new (N)ISASs.
- The potential for gaining synergies in collaboration with other (N)ISASs would be increased with every new national system established.
- New national ISASs would reduce 'white spots' in the security landscape and enhance the overall robustness of the network.

Added value for Member States without national ISASs

- These Member States would be supported in the setting up of their own national ISASs to address their home-users and SMEs from a neutral standpoint.
- They would benefit from the experience of others.
- The establishment and operation of their own ISASs would be much easier.
- New national ISASs would reduce 'white spots' in the security landscape and enhance the overall robustness of the network.

8.3 Foster Dialogue among Existing National ISASs

Added value for Member States with national ISASs

- National ISAS activities in the Member States would gain a facilitating platform for collaboration in order to establish synergies and learn from each other.
- 'Lessons learned' from other national ISASs could be disseminated through meetings and discussions rather than just by documents.
- The development of mutual trust, which is necessary for all kinds of collaboration, would be enhanced by an active dialogue.
- Newly established national ISAS activities could be more easily introduced to their counterparts in other Member States.

Added value for Member States without national ISASs

- These Member States would receive basically the same added value as Member States with existing national ISASs but the action in these cases would have a greater impact.

8.4 Analyse and Review the Practice, Components and Processes to Optimise Information Sharing for the Existing ISASs

Added value for Member States with national ISASs

- Finding synergies (such as for example ‘burden sharing’ in common tasks) could enhance various aspects of existing national ISAS activities including their efficiency, expenses etc.

Added value for Member States without national ISASs

- When the synergies and optimised processes that have been identified have been inserted into the good practice collection, newly established national ISASs would have more optimal procedures and settings available to them from the start; this would bring benefits in a number of areas including finance, acceptance by the target audience etc.

8.5 Proposal of Indicators

The objectives of the potential EISAS, as laid down in the ToR and summarised in 3.1, are:

1. **Raise awareness on NIS issues among European citizens and SMEs**
2. **Assess the added value for existing information sharing activities by enhancing the co-operation among them**

The elaboration of possible ‘indicators to estimate the impact of the shared information’ will be carried out separately for these two objectives.

8.5.1 Raise awareness on NIS issues among European citizens and SMEs

The Expert Group considered assessment of the real impact of an EISAS, in the proposed form, on the status of NIS awareness among (subgroups of) citizens and SMEs nearly impossible to achieve. Several problems are linked with the challenge of measuring the success of the proposed scenario. Firstly, the proposed EISAS (that is a framework for facilitation and the sharing of good practice) does not address home-users and SMEs directly. A success indicator could at the very most be to assess the effect of single (N)ISAS activities on the increase in NIS awareness among the target group(s). But even then it is challenging to measure the success of the information sharing activities in terms of increased awareness, as a recent study by ENISA about the measurement of the success of awareness-raising campaigns proved¹⁰.

The problems begin with the initial measurement of the status quo (“How aware is my target group?”) which is crucial to the evaluation of any increase in awareness. However, the ENISA study identified a number of tools and indicators for measuring the success of awareness-raising campaigns for limited audiences (see table overleaf).



¹⁰ ENISA KPI study – www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf

8 Phase III: Assessment of the Added Value

Metric	Points to consider	Case studies
Number of security incidents due to human behaviour	<p>Can quickly show trends and deviations in behaviour.</p> <p>Can help understand root causes and estimate costs to the business.</p> <p>May not be enough incidents to draw meaningful results.</p> <p>May be other factors that affect the incidents.</p>	<p>Financial services group – page 13</p> <p>Airport operator – page 15</p> <p>Public department – page 18</p>
Audit findings	<p>Generally conducted by independent and knowledgeable people who can provide third party assurance on behaviours.</p> <p>May be significant areas of awareness not reviewed.</p>	<p>International finance services group – page 7</p> <p>Airport operator – page 15</p>
Results of staff surveys	<p>If used before and after specific training, can be used to gauge the effectiveness of campaigns.</p> <p>If sufficiently large, can provide statistical conclusions on staff behaviours.</p> <p>Need to be targeted at verifying key messages.</p> <p>Have to be carefully designed since staff may respond with 'expected' answers and not true behaviours.</p>	<p>International insurer – page 6</p> <p>International airline – page 9</p> <p>Telecommunications provider – page 10</p> <p>Retailer – page 12</p> <p>Government – page 16</p>
Tests of whether staff follow correct procedures	<p>Very good way of actually measuring behaviours and highlighting changes after training.</p> <p>Have to be carefully planned and carried out since could be breaches of employment and data protection laws.</p> <p>Need a big enough sample if results are to be meaningful.</p>	<p>International commercial bank – page 17</p> <p>Public department – page 18</p>
Number of staff completing training	<p>Need to decide what combination of classroom and computer-based training to use.</p> <p>Have to consider what training to make mandatory.</p> <p>May need to be tailored for different areas or regions.</p> <p>May need regular and potentially costly updates.</p>	<p>International finance services group – page 7</p> <p>Retailer – page 12</p> <p>Law enforcement agency – page 13</p> <p>International commercial bank – page 17</p>

Figure 21. Measuring the success of awareness-raising campaigns

A key finding of the ENISA study was that there is no measurement for the success of awareness-raising campaigns (yet), although several procedures have been developed to address the problem at some level.

However, based on experience, it is safe to say that properly functioning systems at a national level that are well advertised and cover the most vulnerable users would add value to the overall robustness of the network. The events that took place in Estonia at the end of April 2007 (large scale botnet DDoS attacks on government, banking and media servers) might suggest that, if more home-users around the world were aware of NIS issues, fewer computers might be herded into botnets and therefore any cyber attacks carried out via botnets would be less harmful.

The absence of clear KPIs however, should not be a reason to abandon activity and research in this area!

8.5.2 Assess the added value for existing information sharing activities by enhancing the co-operation between them

Based on the parameters of added value for Member States with or without their own (N)ISASs, defined earlier in this chapter, it is possible to propose a number of indicators for the success of enhanced co-operation:

- number of newly created (N)ISASs with EU facilitation
- consequent increase in the percentage of EU citizens and SMEs that are covered by an (N)ISAS
- number of existing (N)ISASs that contribute to the EU good practice and facilitation framework
- number of examples of good practice contributed to the clearing house
- number of examples of good practice applied by an existing (N)ISAS ('Learning from others')
- number of fields of improvement ('synergies') found during discussions with existing (N)ISASs
- resulting amount of work (i.e. hours spent daily) that could be saved by a (N)ISAS (statistical average over all existing (N)ISASs)

It should be left to the (N)ISAS community group assembled during the proof of concept phase (see 9.2) to elaborate further on the list of success indicators.

This chapter contains proposals for the European Commission on how to potentially follow up on this study.

9.1 Start Small, but Think Big

Before recommending next steps, it should be stressed that the maxim 'Start small, but think big' is valid in all areas of activity that the European Union might conduct, in order not to raise the expectations of stakeholders too high. The underlying goal should be to reduce the complexity of the proposed solution as much as possible. This is especially true for the kind of information that is shared, as the more immediate the information, the more crucial its timely delivery will become, and problems such as different time zones and different times of operation might arise. This might become a serious obstacle even in an early phase (which has been demonstrated by the EWIS project) unless addressed properly from the start. It is clear therefore that a newly established national ISAS would be best to start with the sharing of good NIS practice information; operating with more time-critical information (such as alerts and warnings) should be considered at a later stage when the new ISAS has been up and running for a while.

It is very easy to list the potential benefits of 'fostering the dialogue among the national ISASs' but, in order to be really successful, this dialogue must aim at realistic and achievable goals. For this reason, activities in the proposed framework should probably start by limiting the target groups to citizens and only after recording some achievements with them (such as a complete basic set of good practices, or a successful pilot for a new national ISAS) should they start thinking about targeting information sharing and alerting at other groups. The same is true for supporting new national ISASs in Member States that do not yet have such a facility and for the 'proof of concept' (PoC) proposed later in this chapter. While it is necessary to hold discussions with all relevant stakeholders about the role that the European Union should play, the number of involved parties in that first PoC should be limited and carefully selected. When this (small-scale) proof of concept activity has shown that it works successfully and has produced genuine added value, larger activities involving more stakeholders and perhaps aiming at more ambitious goals should be planned. (Section 9.2 contains further elaboration on a proposed 'proof of concept'.)

9.2 Proof of Concept

This section outlines a potential 'proof of concept'. One goal is to initiate the activities linked to the proposed EISAS scenario; another is to produce applicable information for follow-up activities.

9.2.1 Concept

In order to demonstrate the feasibility of the proposed EISAS scenario, a 'proof of concept' should be initiated. This would mean assembling a small group of experts, drawn from existing (N)ISAS activities, (see 9.2.2 below) to work in a number of meetings facilitated by the European Union on a set of deliverables (see 9.2.3), taking into account as much existing material and expertise as possible (see 9.2.4). The 'proof of concept' should prove that co-operation between existing (N)ISAS activities both produces comprehensive results and also lays the basis for future work in that area. In particular, it facilitates the setting up of new (N)ISASs in the Member States and the improvement of existing activities through 'learning from each other'.

The group, once assembled, should work independently and be responsible only to itself; however, to assist the process, this section offers suggestions as to how it might proceed.

9.2.2 Assembling the initial group

Following the concept of 'Start small, think big', initially the group should consist of a few (three or four) carefully selected representatives of existing (N)ISAS activities. These representatives should be willing and able to contribute significantly to the work required for this 'proof of concept' solution. The following parameters might be used to select the initial group members:

- whether they have existing material that could be adapted and used in the good practice collection
- whether they have experience of transporting the concept of a (N)ISAS to other countries
- whether they have significant experience in addressing citizens and SMEs via suitable channels including the conventional media or special bodies such as WARPs

9 Proposed Next Steps

- whether they have significant experience in running awareness-raising campaigns for citizens and SMEs, including experience in how to adequately address the various groups of end-users.

To embark on the work as smoothly as possible, it would be helpful if the selected group members had already co-operated with each other in previous projects or did so on a more frequent basis in operational work, so that they can make use of existing relationships.

After bringing the group together, it should be left to them to decide about inviting other members to join them or to enlarge the circle of experts.

9.2.3 Proposed tasks for the group to achieve

- **Deliverable D1 – Create and install a formal basis for the co-operation**

The group should formalise their co-operation in this ‘proof of concept’ in a document such as a ‘Memorandum of Understanding’ or ‘Terms of Reference’. In order to facilitate this process, a draft version should be prepared before the first meeting of the group.

- **Deliverable D2 – Prepare an inventory of available material suited to support the tasks of the group**

The group might start by collecting existing material, beginning with material that they had created themselves, in order to obtain an overview of documentation that could be re-used in the good practice collections.

- **Deliverable D3 – Generate a basic set of good practice information on setting up a (N)ISAS**

Using the material compiled in D2 and based on the expertise of the group members, a skeletal structure of a good practice collection for the establishment of a (N)ISAS should be created.

- **Deliverable D4 – Generate a basic set of good practice information on the operation of a (N)ISAS**

Using the material compiled in D2 and based on the expertise of the group members, a skeletal structure of a good practice collection for successfully running a (N)ISASs should be created.

- **Deliverable D5 – Generate a (fictitious) case study on how a new (N)ISAS in a Member State might be installed**

The case study should act as a guideline on how the good practices collected and recorded in D3 and D4 might be applied ‘in the field’. A promising structure for this might be derived from ENISA’s guide “A step by step approach on how to set up a CSIRT”¹¹, which also includes a project plan, and has already proved its practicability in several cases.

- **Deliverable D6 – Make a proposal for promising follow-ups**

Based on its findings and the results of discussions held while completing its tasks, the group should conclude with a simple roadmap containing advice and guidelines on how to proceed with future activities. The roadmap should also make a proposal for the further involvement of the European Union, taking into account the possibilities of the facilitating roles laid down in 9.3.

- **Deliverable D7 – Workshop**

The results produced in the ‘proof of concept’ and the findings of the group could be presented in a workshop for the stakeholders that could be facilitated by the European Union.

9.2.4 Proposal of material to be taken into account

This section contains details of material prepared by existing (N)ISAS activities and other competent bodies that should be taken into account by the participants in this ‘proof of concept’.

- **ENISA’s deliverables**

Sections 4.3 and 4.4 contain details of relevant ENISA deliverables.

¹¹ ENISA CSIRT setting-up guide – www.enisa.europa.eu/cert_guide/index_guide.htm

- **WARPs**

Short explanation:

WARPs (Warning, Advice and Reporting Points) are part of CPNI's information sharing strategy to protect the UK's Critical National Infrastructure from electronic attack. WARPs have been shown to be effective in improving information security by stimulating better communication of alerts and warnings, improving awareness and education, and encouraging incident reporting. Membership of a WARP can also reduce the costs of good security.

WARP members agree to work together in a community and share information to reduce the risk of their information systems being compromised, thereby reducing the risk to their organisations. This sharing community could be based on a business sector, geographic location, technology standards, risk grouping or whatever makes business-sense.

WARPs can deliver more effective and lower cost security by providing members with:

- A trusted environment
- Security information filtering
- Access to expert advice
- Early warning of threats
- Strategic decision support
- Improved awareness

WARPs are currently established in the following sectors: Local Government, SMEs, Voluntary, Home-users, Emergency Services and Managed Service Providers, but are suitable for all types of communities.

Assessment:

The WARP concept is a very interesting model of how to transport NIS-related information as close to the end-user as possible. The information is delivered inside a trusted community of users with similar levels of expertise. As the concept, developed in the UK, is slowly taken up by information sharing activities in other Member States, the WARP concept should definitely be considered as a valuable contribution to the good practice collection to be developed during this 'proof of concept'.

More information: www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

- **Be Informed Warned Aware**

Short explanation:

The German BSI developed a brochure with explanations as to how to successfully build up an information sharing service for citizens. Together with a CD that contains a live demonstration of the 'BuergerCERT Online System (BCOS)', the brochure was distributed at the IT Security Conference of the German EU Council Presidency on 4 and 5 June 2007. Neither the brochure nor the CD are available on the Internet at the time of writing.

Assessment:

The BSI brochure could serve as a basis for the creation of the good practice collection in this 'proof of concept'. Together with the CD that contains tools and tips to facilitate the initiation of (N)ISAS activities, the material prepared by the German CERT-BUND/BSI is first class and makes a valuable contribution to the good practice collection.

More Information:

Federal Office for Information Security (BSI), Section 321 – Information and Communication, Public Relations.

- **Alerting-Service-in-a-box (part of CERT-in-a-box)**

Short explanation:

'CERT-in-a-Box' and 'Alerting service-in-a-Box' are part of an initiative of GOVCERT.NL to preserve the lessons learned from setting up GOVCERT.NL and 'De Waarschuwingsdienst', the Dutch national alerting service.

9 Proposed Next Steps

The project aim is to help others starting a CSIRT or an alerting service by:

- Helping them to make progress as quickly as possible
- Passing on the benefits of the Dutch experience.

Assessment:

This case study on how to successfully set up and run an Information Sharing and Alerting Service for citizens, SMEs and others should definitely be considered as a valuable contribution to the good practice collection to be developed during this 'proof of concept'.

More information: www.enisa.europa.eu/cert_inventory/pages/04_02.htm#02

9.2.5 Potential follow-ups

Investigate further how to address home-users and SMEs

One of the findings of this study was that NIS-related information must be provided in special ways to reach out effectively to home-users and SMEs (native language, no 'tech talk', no information overflow etc.). In the discussions that took place with the Expert Group, it was established that technical experts find it difficult to explain highly technical issues in a way that is understood by home-users and SMEs. This makes adequate information sharing with these target groups a real challenge. How to address non-technical users so that they understand and embrace the necessity of using the Internet responsibly is a field that should be explored further.

It is recommended that ways of conveying NIS-related information to non-experts such as home-users and SMEs should be explored. Work already accomplished in this area should be taken into account, as a number of projects and activities have already been conducted which successfully communicate NIS matters to home-users and SMEs. ENISA has also completed relevant work. The Awareness-Raising information packages and the forthcoming study into "User needs for CERT services" are just two examples. ENISA could, on request, develop a plan to approach this issue, manage the contacts to the various activities in the field and collect examples of good practice.

9.3 The Potential Role of ENISA

This section lists ENISA's capabilities and prospects and highlights the potential roles that the Agency, together with the European Commission, could play in the field of EISAS. Some of these roles might usefully be combined.

9.3.1 ENISA's position

The regulation governing ENISA's establishment¹², paragraph 'Scope' (Article 1) states:

"The Agency shall assist the Commission and the Member States, and in consequence co-operate 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."

The same regulation, paragraph 'Objectives' (Article 2) states:

"The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems."

The Agency shall provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security falling within its competencies as set out in this 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 co-operation between actors from the public and private sectors."

Potential role: To act as an independent and competent centre of expertise; to act as an independent moderator (or mediator) during the discussions between the existing (national) ISAS activities.

¹² Regulation (EC) No. 460/2004 - http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32004R0460&model=guicheti

9.3.2 European NIS Good Practice Brokerage

A limited number of Member States already work together to exchange experiences in order to develop and improve their NIS capabilities. To enhance the level of NIS on a European basis, all Member States should be encouraged to share information on good practices on a structured basis.

ENISA initiated a European 'NIS Market Place' in 2007 and will act as a broker between those Member States that have developed good practices in certain NIS areas and are willing to share them and those Member States that want to learn about particular experiences. For example, in 2007, the Good Practice Brokerage facilitated co-operation between CERT-Hungary and the Bulgarian Telecommunication Authority over the setting up of BL-GOVCERT.

ENISA considers this a long term and continuous task as Member States need to be introduced to the potential of co-operation and to be convinced that co-operation would be fruitful and beneficial for all partners. An annual review will be conducted in order to evaluate and obtain feedback on the functioning of the European NIS Good Practice Brokerage scheme.

Potential role: As a clearing house of good practice information about the setting up and running of new national ISASS; as a facilitator for the process of setting up and running new national ISASSs.

9.3.3 Network of NLOs

ENISA has set up a network of National Liaison Officers (NLOs). Although not formally based on the ENISA Regulation, this network is of great value and importance to ENISA as the NLOs serve as ENISA's primary contact with the Member States. On the other hand, ENISA offers the NLOs an opportunity to reinforce the activity of the Agency in the Member States and to exchange information amongst themselves. Based on the input from the Member States (through the National Liaison Officers), ENISA has set up and is maintaining 'Country Pages' on its website to inform stakeholders about points of contact and activities in the Member States. ENISA can quickly retrieve and deliver information directly from and to primary NIS focal points in the Member States.

Potential role: As a facilitator of the dialogue with the Member States.

9.3.4 PSG

The Permanent Stakeholders' Group (PSG) is a group of leading experts which acts as a sounding board for and advises the Executive Director of ENISA on the drawing up of the Agency's work programme, as well as in ensuring communication with relevant stakeholders on all issues related to the work programme. For example, the PSG has contributed its views on the ENISA Work Programme for 2007 and its longer-term vision of future activities.

The PSG is composed of 30 high-level experts from all over Europe. Although appointed ad persona, they represent the relevant stakeholders, such as the information and communication technologies industry, consumer groups and academic experts in network and information security.

Potential role: As a facilitator of the dialogue with the stakeholders from the private sector.

9.3.5 Ad hoc WG

The Executive Director of ENISA has powers to set up ad hoc working groups to address specific scientific and technical matters. These groups should be competent and representative and should include, where appropriate to the specific issues under consideration, representatives of the public administrations of EU Member States, the private sector including industry, users and academic experts in NIS. Each group comprises between five and nine leading NIS experts in relevant areas. In establishing ad hoc working groups, ENISA seeks to obtain input from the private sector and to mobilise its expertise.

Members of ad hoc working groups are appointed by the Executive Director of ENISA from lists drawn up following open calls for expressions of interest from leading experts in particular technical and scientific matters related to NIS. The need for a new working group may be recommended to the Executive Director by ENISA's Management Board or by the Permanent Stakeholders' Group.

9 Proposed Next Steps

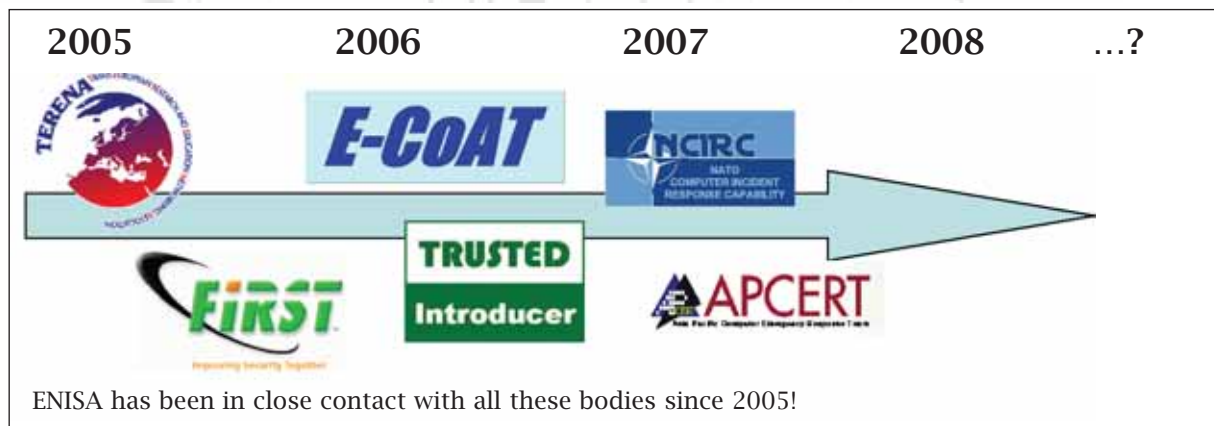
Ad hoc working groups should provide a final report at the end of their mandate. If their activities exceed six months, groups must prepare an intermediate report. Reports and opinions by ad hoc working groups are communicated to the Executive Director, who then forwards them for information to the Chairperson of the Management Board.

Expenses incurred in connection with the activities of ad hoc working groups, including the travel and subsistence expenses of experts, are reimbursed by ENISA.

Potential role: Together with experts, as a facilitator in the process of collecting new examples of good practice, based on synergies and areas of potential improvement identified during the dialogue between the existing ISASs in the Member States.

9.3.6 CERT contacts

Right from the Agency's establishment, ENISA's CERT experts have been in close contact with all relevant CERT (and similar) communities in Europe and beyond. For example, ENISA's experts attend the meetings of the Terenas Task-FORCE CSIRT (TF-CSIRT) on a regular basis and have facilitated TRANSITS training organised by this community. ENISA's CERT experts also enjoy (liaison) membership in the worldwide FIRST organisation (Forum of Incident Response and Security teams) and jointly with FIRST organised the 19th Annual FIRST conference in Sevilla, Spain in 2007. These experts are well known and respected among the various CERT (and similar) communities and have a distinguished network of contacts with CERTs worldwide. In addition, ENISA's CERT experts work or have worked in CERTs for several years and are involved in information sharing activities for various stakeholders.



ENISA and the CERT communities

Potential role: As a facilitator of the discussion with the CERT (and similar) communities.

9.3.7 Present and future deliverables from ENISA

The ENISA Inventory of CERT activities in Europe

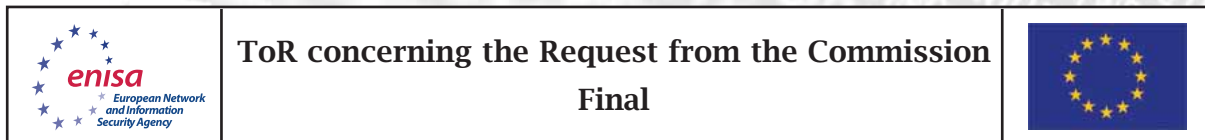
This Inventory lists all relevant co-operation activities in Europe and beyond that might potentially be important for the proposed EISAS scenario, independently of the eventual shape of that scenario.

The ENISA Study on CERT Co-operation and its Further Facilitation

In 2006 ENISA produced a study that analysed the vast field of co-operation among CERT/CSIRTs and similar bodies. It was the first document of its kind, and not only tells the story of co-operation in Europe and beyond, but also summarises the lessons learned and makes recommendations to the stakeholders involved as to how co-operation might be improved. This study can therefore be used as a starting point for planning the next steps that might be taken as a follow-up to this current EISAS study.

Other deliverables produced during 2007/2008 might also be used to set up a stock of good practice information on how to set up and run a (national) ISAS.

Potential role: As a provider of content to the good practice collection; as a facilitator of the process of identifying synergies and fields of improvement in the existing ISAS activities by injecting expertise into the discussions among these activities.



Examining the feasibility of a EU-wide information sharing and alert system

Background

In its COM(2006) 251, the Commission emphasises that public authorities, in Member States and at EU-level, have a key role to play in properly informing users to enable them to contribute to their own safety and security: “In order to improve the European capability to respond to network security threats” means “to facilitate effective responses to existing and emerging threats to electronic networks” should be explored. This need is being matched by the Commission’s request to ENISA “to examine the feasibility of a European information sharing and alert system” (Section 3.2.2). In so doing, the Commission highlights the role of ENISA in fostering a culture of security in Europe.

Scope and Objectives

One of the main objectives of fostering a culture of security is **raising awareness on NIS issues** and providing appropriate and timely information on threats, risks and alerts as well as on good practices. To this end, the primary responsibility of MS in carrying out these activities to improve national capabilities to respond to NIS threats according to their national NIS and related policies is acknowledged. However, better cooperation among MS might add value to those single initiatives. Against this background, the aspect of promoting the exchange of information and lessons learnt among MS could help achieve the overall goal (enhancing NIS in the EU). The task is primarily targeting at citizens and SMEs (but network operators and service providers should not be excluded at this point in time).



The expected result is a recommendation whether and if so, how an EU-wide system could be realized by combining existing MS’ systems.

Approach to be taken

The approach to the requested task comprises 3 activities: (1) **analyzing the current state of affairs** in public and private sector, (2) **examining the feasibility** of such a European Information Sharing and Alert System (EISAS) including a multilingual EU portal and (3) **assessing its added value** to effectively react to NIS threats and efficiently support citizens and SMEs.

The activities would normally build upon and link together existing/planned MS initiatives and initiatives of other stakeholders. ENISA would carry out the activities in close cooperation with MS and other stakeholders who are currently managing related initiatives. This would emphasise the collective effort needed by MS and European stakeholders to accomplish the objective of the study. To this end, ENISA would examine existing initiatives and possible sources of security information that can potentially contribute to an EISAS. A part of the study would be an inventory of available sources as well as an inventory of work done so far (for instance, BuergerCERT in Germany, Waarschuwingsdienst in The Netherlands, the WARP activities in UK, etc.) whereas language issues have to be taken into account, too.

Annex A: The Terms of Reference

	ToR concerning the Request from the Commission Final	
---	---	---

(1) Analyzing current state of affairs

- Collect information about existing information sharing and alerting systems and compile an inventory
- Collect information about sources of security related information available (both free and commercial sources) and compile an inventory
- Establish a group of experts from MS governments and other stakeholders that are experienced in running Information Sharing activities that ENISA can consult in carrying out the activity.

(2) Examining the feasibility of an EISAS

The following steps are proposed to conduct in close cooperation with the MS, e.g. by convening the above mentioned networks of expert contacts in (virtual and physical, as appropriate) meetings, etc:

- Conduct an analysis of the inventory of work done so far in terms of
 - The nature of the shared/ distributed information (dynamic information, static information, real time information)
 - The rationale behind these different national approaches (considering targets, functionality etc.)
 - The content of the shared information
 - The target group for this information
 - Information exchange mechanisms (exchange formats)
 - Other factors
- Conduct an analysis of the inventory of available sources in terms of
 - The nature of the security information (Real time alerts, security advisories, good common practice)
 - Availability (Copyright, License)
 - Potential contribution to an EISAS
 - Other factors
- Describe a possible scenario (or different scenarios if the analysis shows that there exist several models) for an EISAS, taking into account the two analyses, including the requirements, nature of shared information and target group.

(3) Assessing the added value of an EISAS

This activity should comprehend two steps:

- An analysis of whether and how the to-be concept EISAS would contribute to as-is solutions as well as could improve the overall security culture in Europe (e.g. by addressing new target groups that were not covered before).
- A proposal of indicators that can be used to estimate the impact of the shared information (i.e. total numbers of incidents in the target groups).
- Validate the findings in a workshop with MS governments and other relevant stakeholders.

Timeline (major milestones)

ENISA will start these activities in October 2006 and finish this request in June 2007 with a view to present the final results at the e-security conference organised by the German Presidency. Intermediate results will be discussed and validated in a workshop to be held between March and April 2007.

Annex B: Inventory of Systems

It should be noted that not all of the systems included in the inventory are already in a productive state. Some of them only exist in theory; others are in a pilot phase or near completion.

Part I: Type of Information, Language, Maintainer and Channels

System Name	Location (Member State)	Type of Information	Language	Maintainer	Distribution Channels
Internet Analysis System	GE	Real-time	German	Fachhochschule Gelsenkirchen	www
ARAKIS	PL	Real-time	Polish, English	CERT Polska/ NASK	www, e-mail
ARGOS	NL	Real-time	Dutch	Vrije Universiteit Amsterdam	
BSI fuer Buerger	GE	Good NIS practice	German	BSI/CERT-Bund	www, e-mail
Buerger CERT	GE	Alerts & Warnings	German	BSI/CERT-Bund	www, e-mail
CarmentiS	GE	Real-time	German	CERT-Verbund	www, e-mail
CASES.lu	LU	Good NIS practice, Alerts & Warnings	French	Ministère de l'Économie et du Commerce extérieur	www
CERT-EE	EE	Good NIS practice, Alerts & Warnings, Real-time	Estonian, English	CERT EE	www, e-mail, SMS, IM, RSS
CERT-FI	FI	Good NIS practice, Alerts & Warnings	Finnish, English	CERT-FI	www, e-mail
CERT-PT	PT	Good NIS practice, Alerts & Warnings	Portuguese, English	CERT.PT - Lino Santos	www, e-mail
CIRCA	AT	Alerts & Warnings, Real-time	German, English	BKA (Federal Chancellor's Head Office), ISPA (Internet Service Providers, Austria)	www, e-mail
COSSI	FR	Good NIS practice, Alerts & Warnings, Real-time	French	SGDN/DCSSI	www, mailing list, fax, mail, phone
CyTRAP Labs - CASEScontact.org	EU	Good NIS practice, Alerts & Warnings	English, German	Urs E. Gattiker	www, e-mail, RSS
DeWorm/Sentinels	NL	Real-time	Dutch, English	Vrije Universiteit Amsterdam	www
DK-CERT Vulnerability Database	DK	Good NIS practice, Alerts & Warnings	Danish	DK-CERT	www, e-mail
EAR	GR	Real-time	English	FORTH	
Esaugumas	LT	Alerts & Warnings	Lithuanian	Communications Regulatory Authority of the Republic of Lithuania	www, e-mail

Annex B: Inventory of Systems

System Name	Location (Member State)	Type of Information	Language	Maintainer	Distribution Channels
German Honeynet Project	GE	Real-time	German/English	Aachen University	
GetSafeonLine	UK	Good NIS practice	English	CPNI	www, e-mail
IT Safe	UK	Alerts & Warnings	English	CPNI	www, e-mail, RSS
Leurre.Com	FR	Real-time	English	EURECOM	www
LOBSTER	UE	Real-time	English	FORTH (GR), Vrije Universiteit Amsterdam (NL), CESNET (CZ), UNINETT (NO), Endace (UK), Alcatel CIT (FR), FORTHnet (GR), TNO Telecom (NL), TERENA (NL)	www
Deutschland sicher im Netz	GE	Good NIS practice	German	BMI	www, e-mail
MELANI	CH	Good NIS practice, Alerts & Warnings, Real-time	German, French, Italian, English	CERT-SWITCH	www, e-mail
NOAH	EU	Real-time	English	FORTH (GR), Alcatel CIT (FR), DFN-CERT (DE), ETH (CH), FORTHnet (GR), TERENA (NL), Virtual Trip Ltd (GR), Vrije Universiteit Amsterdam (NL)	
NORCERT	NO	Real-time	Norwegian	VDI	www, e-mail
NORSIS	NO	Good NIS practice, Alerts & Warnings	Norwegian	NORSIS	www
Proventia	LV	Real-time	English	VITA CSIRT	www, e-mail
Security AR portal	EE	Good NIS practice, Alerts & Warnings	Estonian	Vaata Maailma S.A.	www, campaigns
Sitic - Swedish IT Incident Centre	SE	Good NIS practice, Alerts & Warnings, Real-time	Swedish	Swedish Government	www, e-mail
SURFnet IDS	NL	Real-time	English	SURFnet	www
Waarschuwingsdienst	NL	Good NIS practice, Alerts & Warnings	Dutch	GOVCERT.NL	e-mail lists, www, SMS, media, press
WARPs	UK	Good NIS practice, Alerts & Warnings	English	CPNI	own distribution method

Annex B: Inventory of Systems

Part II: Target Group, Sources and Conditions of Use

System Name	Location	Target group	Sources of information used	Conditions of use
Internet Analysis System	GE	project members	sensor network	closed
ARAKIS	PL	various PL institutions	publicly available information, sensor network	partly open
ARGOS	NL	project members	sensor network	closed
BSI fuer Buerger	GE	citizens, SMEs	publicly available information (commercial, free)	open
Buerger CERT	GE	citizens, SMEs	publicly available information (commercial, free)	open
CarmentiS	GE	project members	sensor network	closed
CASES.lu	LU	citizens, SMEs	publicly available information, information provided by CASES	partly open
CERT-EE	EE	CIIP focussed (end-users planned)	crafted and vendor advisories	open
CERT-FI	FI	Finnish public	publicly available information (commercial, free)	open
CERT-PT	PT	Portuguese public	publicly available information	open
CIRCA	AT	project members	publicly available information (commercial, free)	closed
COSSI	FR	public administration (citizens, SMEs planned)	publicly available information	closed
CyTRAP Labs - CASEScontact.org	EU	home-users, SME, media	publicly available information, own research	open
DeWorm/Sentinels	NL	project members	sensor network	closed
DK-CERT Vulnerability Database	DK	Danish public	publicly available information	open
EAR	GR	project members	sensor network	closed
Esaugumas	LT	Lithuanian public	publicly available information	open
German Honeynet Project	GE	project members	sensor network	closed
GetSafeonLine	UK	citizens, SMEs	publicly available information, own research	open
IT Safe	UK	citizens, SMEs	publicly available information, own research	open
Leurre.Com	FR	project members	sensor network	closed
LOBSTER	UE	project members	sensor network	closed
Deutschland sicher im Netz	GE	citizens, SMEs	publicly available information, own research	open
MELANI	CH	mainly CIIP focussed	sensor network, publicly available information	partly open
NOAH	EU	project members		closed
NORCERT	NO	mainly CIIP focussed	sensor network, publicly available information	partly open
NORSIS	NO	Norwegian public	publicly available information	open
Proventia	LV	gov.lv, municipalities	publicly available information	partly open
Security AR portal	EE	citizens, SMEs	publicly available information	open
Sitic - Swedish IT Incident Centre	SE	Swedish public authorities, councils, municipalities, companies	publicly available information (commercial, free)	partly open
SURFnet IDS	NL		sensor network, publicly available information	partly open
Waarschuwingsdienst	NL	SMEs, citizens	publicly available information	partly open
WARPs	UK	small communities	CPNI-advisories	n/a

Annex B: Inventory of Systems

Part III: Web Address, Revenue Model and CERT Involvement

System Name	Location	www page	Revenue model	CERT involved
Internet Analysis System	GE	www.internet-sicherheit.de/ias-summary.html	research project	
ARAKIS	PL	www.arakis.pl	public-private partnership	Directly
ARGOS	NL	www.few.vu.nl/~porto/argos/	research project	
BSI fuer Buerger	GE	www.bsi-fuer-buerger.de/	public	Indirectly
Buerger CERT	GE	www.buerger-cert.de	public	Directly
CarmentiS	GE	www.cert-verbund.de/carmentis/index.html	public-private partnership (project)	
CASES.lu	LU	www.cases.public.lu/	public	
CERT-EE	EE	www.cert.ee	public	Directly
CERT-FI	FI	www.cert.fi	public	Directly
CERT-PT	PT	www.cert.pt/	NREN	Directly
CIRCA	AT	www.circa.at	public-private partnership	Indirectly
COSSI	FR	n/a	public	Directly
CyTRAP Labs - CASEScontact.org	EU	www.casescontact.org	public-private partnership	
DeWorm/Sentinels	NL	www.cs.vu.nl/~herbertb/projects/deworm/	research project	
DK-CERT Vulnerability Database	DK	www.cert.dk	NREN	Directly
EAR	GR	www.ics.forth.gr/dcs/Activities/Projects/ear.html	research project	
Esaugumas	LT	www.esaugumas.lt	public	Directly
German Honeynet Project	GE	n/a	research project	
GetSafeonLine	UK	www.getsafeonline.org	public	Directly
IT Safe	UK	www.itsafe.gov.uk	public	Directly
Leurre.Com	FR	www.leurrecom.org/	research project	
LOBSTER	UE	www.ist-lobster.org/	research project	
Deutschland sicher im Netz	GE	https://www.sicher-im-netz.de/	public-private partnership	
MELANI	CH	www.melani.admin.ch	public-private partnership	Directly
NOAH	EU	www.fp6-noah.org	research project	
NORCERT	NO	www.cert.no	public	Directly
NORSIS	NO	http://norsis.no/	private	
Proventia	LV		public	
Security AR portal	EE	www.arvutikaitse.ee	public-private partnership	
Sitic - Swedish IT Incident Centre	SE	www.sitic.se	public	Directly
SURFnet IDS	NL	http://ids.surfnet.nl/	NREN	
Waarschuwingsdienst	NL	www.waarschuwingsdienst.nl	public	Directly
WARPs	UK	www.warp.gov.uk/	public	Directly

Annex C: Inventory of Publicly Available Sources

Name	Weblink	Topics	Info Provider	Distribution	Language
Adobe	www.adobe.com/cfusion/entitlement/index.cfm?e=szalert	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Antivirus	http://antivirus.about.com/	Viruses	Commercial/ Vendor	Website	English
Apache	http://httpd.apache.org	Vulnerabilities	Commercial/ Vendor	Website	English
Apache	http://httpd.apache.org/lists.html#http-announce	Vulnerabilities	Non- Commercial	Mailing list	English
Apache	www.apacheweek.com/features/security-13	Vulnerabilities	Commercial/ Vendor	Website	English
Apple	http://docs.info.apple.com/article.html?artnum=61798	Vulnerabilities	Commercial/ Vendor	Website	English
Apple	http://lists.apple.com/mailman/listinfo/security-announce	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Apple - Product Security	www.apple.com/support/security/	Notifications	Commercial/ Vendor	Website	English
Arkoon	www.arkoon.net	Vulnerabilities	Commercial/ Vendor	Website	French, English
AusCERT	www.auscert.org.au/	Vulnerabilities	CERT Academic	Website	English
BEA	http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/index.jsp	Vulnerabilities	Commercial/ Vendor	Website	English
BELNET CERT	http://cert.belnet.be	Vulnerabilities	CERT	Website	English
BugTraq	www.securityfocus.com/archive	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Business objects	http://support.businessobjects.com/fix/hot/critical/default.asp	Vulnerabilities	Commercial/ Vendor	Website	English
CA	http://supportconnectw.ca.com	Vulnerabilities	Commercial/ Vendor	Website	English
Canadian Cyber Incident Response Centre	www.ps-sp.gc.ca/prg/em/ccirc/index-en.asp	Vulnerabilities	Government	Website	English, French
CERT BUND	www.bsi.bund.de/certbund	Vulnerabilities	CERT (gov)	Website	German
CERT Estonia	www.cert.ee	Vulnerabilities	CERT	Website	Estonian
CERT FI	www.cert.fi	Vulnerabilities	CERT	Website	Finnish
CERT Hungary	www.cert-hungary.hu	Vulnerabilities	CERT	Website	Hungarian
Cert IST	www.cert-ist.com/	Vulnerabilities	CERT - Commercial/ Vendor	Mailing lists, website, discussion lists, RSS- feeds	French, English
CERT LEXSI	www.lexsi.com	Vulnerabilities	CERT	Website	French
CERT Polska	www.cert.pl	Vulnerabilities	CERT	Website	Polish
CERT.PT	www.cert.pt	Vulnerabilities	CERT	Website	Portuguese
CERT/CC	www.cert.org/	Vulnerabilities	CERT Academic	Website	English

Annex C: Inventory of Publicly Available Sources

Name	Weblink	Topics	Info Provider	Distribution	Language
CERT/CC	www.cert.org/other_sources/viruses.html#II	Viruses	CERT Academic	Website	English
CERTA	www.certa.ssi.gouv.fr	Vulnerabilities	CERT (gov)	Website, mailing list	French
Certcom	www.certcom.de/	Vulnerabilities	Commercial/ Vendor	Website	German
CERT-Renater	www.renater.fr/spip.php?rubrique19	Vulnerabilities	CERT	Website, mailing list	French
Checkpoint	www.checkpoint.com/services/mailling.html	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Checkpoint	www.checkpoint.com/techsupport/alerts/	Vulnerabilities	Commercial/ Vendor	Website	English
CIAC - US Department of Energy	www.ciac.org	Vulnerabilities	Government	Mailing list	English
Cisco	www.cisco.com/en/US/products/products_security_advisories_listing.htm	Vulnerabilities	Commercial/ Vendor	Website	English
Cisco	www.cisco.com/en/US/products/products_security_vulnerability_policy.html#subscribe	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Citrix	http://support.citrix.com/latestsecurityall!execute.jspa	Vulnerabilities	Commercial/ Vendor	Website	English
CME	http://cme.mitre.org/data/list.html	Monitoring	Commercial/ Vendor	Website	English
Corsaire	www.corsaire.com/advisories/	Vulnerabilities	Commercial/ Vendor	Website	English
CPNI	www.cpni.gov.uk/	Vulnerabilities	Government	Website	English
CSIRTUK	www.cpni.gov.uk/Products/advisories.aspx	Vulnerabilities	CERT (gov)	Website	English
CVE	https://cassandra.cerias.purdue.edu/CVE_changes/	Vulnerabilities	Commercial/ Vendor	Website	English
CybSec	www.cybsec.com/ES/noticias/default.php	Vulnerabilities	Commercial/ Vendor	Website	Spanish
dCERT	www.dcert.de	Vulnerabilities	CERT	Website	German/ English
DFN-CERT	www.dfn-cert.de/infoserv/mls/win-sec-ssc.html#TOPIC	Vulnerabilities	CERT	Security advisories	English
DK CERT	www.cert.dk	Vulnerabilities	CERT	Website	Danish
dShield	http://dshield.org/	Status Monitoring	Commercial/ Vendor	Website	English
eEye	www.eeye.com/html/index.html	Status Monitoring	Commercial/ Vendor	Website	English
EISPP Project	www.eispp.org/	Awareness-raising	Academic	Mailing list	English
ESACERT	www.esacert.esa.int	Vulnerabilities	CERT	Website	German
esCERT-UPC	http://escert.upc.es	Vulnerabilities	CERT	Website	Spanish
Fedora Legacy	www.fedoralegacy.org/updates/FC1/	Vulnerabilities	Commercial/ Vendor	Website	French, English

Annex C: Inventory of Publicly Available Sources

Name	Weblink	Topics	Info Provider	Distribution	Language
Fedora Legacy	www.fedoralegacy.org/updates/	Vulnerabilities	Website	Website	French, English
FIRST	www.first.org/	General information	Mailing list	Mailing list	English
FIRST NEWS	www.first.org/newsroom/globalsecurity/	Vulnerabilities, Awareness-raising	Commercial/Vendor	Mailing list	English
FreeBSD	www.freebsd.org/security/index.html	Vulnerabilities	Commercial/Vendor	Website	English
FreeBSD	http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications	Vulnerabilities	Non-Commercial	Mailing list	English
F-Secure	http://support.f-secure.com/enu/corporate/downloads/hotfixes/	Vulnerabilities	Commercial/Vendor	Website	English
F-Secure	www.f-secure.com/products/radar/alerts/	Vulnerabilities	Commercial/Vendor	Website	English
F-Secure	www.f-secure.com/security/	Vulnerabilities	Commercial/Vendor	Website	English
F-Secure	www.f-secure.com/security_center/	Vulnerabilities	Commercial/Vendor	Website	English
F-Secure	www.f-secure.com/v-descs/_new.shtml	Viruses	Commercial/Vendor	Website	English
Full Disclosure	http://lists.grok.org.uk/full-disclosure-charter.html	Vulnerabilities	Non-Commercial	Mailing list	English
GARR CERT	www.cert.garr.it	Vulnerabilities	CERT	Website	Italian
GOVCERT.IT	www.govcert.it	Vulnerabilities	CERT (gov)	Website	Italian
GOVCERT.NL	www.govcert.nl	Vulnerabilities	CERT (gov)	Website	Dutch
GRNET CERT	http://cert.gmet.gr	Vulnerabilities	CERT	Website	Greek
HP	www.hp.com	Vulnerabilities	Commercial/Vendor	Mailing list	English
IBM	www.ibm.com	Vulnerabilities	Commercial/Vendor	Mailing list	English
Idefense	www.idefense.com/	Status monitoring	Commercial/Vendor	Website	English
ISS	https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp	Internet activity monitoring	Commercial/Vendor	Website	English
ISS	http://xforce.iss.net/xforce/maillists/	Vulnerabilities	Commercial/Vendor	Mailing list	English
ISS XForce	http://xforce.iss.net/	Vulnerabilities	Commercial/Vendor	Website	English
Juniper	www.juniper.net/support/security/security_notices.html	Vulnerabilities	Commercial/Vendor	Website	English
KB US-CERT	www.kb.cert.org/vuls	Vulnerabilities	CERT (gov)	Website	English
KPN-CERT	www.kpn-cert.nl	Vulnerabilities	CERT	Website	English
Linux Debian	http://lists.debian.org/debian-security-announce/	Vulnerabilities	Commercial/Vendor	Mailing list	English
Linux Fedora	www.redhat.com/mailman/listinfo/fedora-package-announce	Vulnerabilities	Commercial/Vendor	Mailing list	English

Annex C: Inventory of Publicly Available Sources

Name	Weblink	Topics	Info Provider	Distribution	Language
Linux Fedora Legacy	www.fedoralegacy.org/mail/	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Linux Kernel	www.kernel.org	Vulnerabilities	Commercial/ Vendor	Website	English
Linux Mandriva	www.mandriva.com/en/community/resources/ node_838#security	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Linux Red Hat	https://www.redhat.com/archives/enterprise- watch-list/	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Linux Slackware	www.slackware.com/lists/	Vulnerabilities	Non- Commercial	Mailing list	English
Linux SuSE	www.novell.com/linux/security/securitysupport. html	Vulnerabilities	Commercial/ Vendor	Website	English
Linux SuSE	suse-security-announce-subscribe@suse.com	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Linux Trustix	http://lists.trustix.org/mailman/listinfo/ tsl-announce	Vulnerabilities	Commercial/ Vendor	Mailing list	English
LITNET CERT	http://cert.litnet.lt	Vulnerabilities	CERT	Website	Lithuanian
Lotus	http://www-10.lotus.com/ldd/security	Vulnerabilities	Commercial/ Vendor	Website	English
Macromedia	www.adobe.com/cfusion/entitlement/index. cfm?e=szalert	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Macromedia	www.macromedia.com/v1/developer/ securityzone/securitybulletins.cfm	Vulnerabilities	Commercial/ Vendor	Website	English
McAfee	http://vil.nai.com/vil/signup_DAT_ notification. aspx	Viruses	Commercial/ Vendor	Mailing list	English
mCERT	www.mcert.de	Vulnerabilities	CERT	Website	German
MessageLabs	www.messageLabs.com	Viruses	Commercial/ Vendor	Website	English
Micro-BIT	www.rz.uni-karlsruhe.de/rd/microbit.php	Vulnerabilities	CERT	Website	German
Microsoft	www.microsoft.com/technet/security/advisory/ default.mspx	Vulnerabilities	Commercial/ Vendor	Website	English
Microsoft	www.microsoft.com/technet/security/bulletin/ notify.mspx	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Mozilla	www.mozilla.org/projects/security/known- vulnerabilities.html#mozilla1.7	Vulnerabilities	Commercial/ Vendor	Website	English
mtCERT	www.mtcert.gov.mt	Vulnerabilities	CERT	Website	Maltese
Nagios	www.nagios.org/development/changelog.php	Vulnerabilities	Commercial/ Vendor	Website	English
NAI	http://vil.nai.com/vil/newly_discovered_viruses. aspx	Viruses	Commercial/ Vendor	Website	English
NAI	www.nai.com/us/downloads/updates/hotfixes. asp	Vulnerabilities	Commercial/ Vendor	Website	English
NetASQ	www.netasq.com/en/index.php	Vulnerabilities	Commercial/ Vendor	Mailing list	French, English
NetBSD	www.netbsd.org/fr/MailingLists/#netbsd- announce	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Netscape	http://browser.netscape.com/ns8/security/ alerts.jsp	Vulnerabilities	Commercial/ Vendor	Website	English

Annex C: Inventory of Publicly Available Sources

Name	Weblink	Topics	Info Provider	Distribution	Language
NIST	http://csrc.ncsl.nist.gov/	Vulnerabilities	Academic	Website	English
Nortel	http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SECUREADVISORY	Vulnerabilities	Commercial/ Vendor	Website	English
Novell	http://support.novell.com/filefinder/security/index.html	Vulnerabilities	Commercial/ Vendor	Website	English
Novell	www.novell.com/company/subscribe/	Vulnerabilities	Commercial/ Vendor	Mailing list	English
NTA Monitor	www.nta-monitor.com/news/nta-in-news.htm	Vulnerabilities	Commercial/ Vendor	Website	English
NTBugTraq	www.ntbugtraq.com/	Vulnerabilities	Commercial/ Vendor	Mailing list	English
OpenBSD	www.openbsd.org/errata.html	Vulnerabilities	Commercial/ Vendor	Website	English
Oracle	http://otn.oracle.com/deploy/security/alerts.htm	Vulnerabilities	Commercial/ Vendor	Website	English
Oracle (unofficial)	www.petefinnigan.com/alerts.htm	Vulnerabilities	Commercial/ Vendor	Website	English
OSSIR	www.ossir.org/	Vulnerabilities	Academic	Mailing list	French
OSVDB	www.osvdb.org	Vulnerabilities	Commercial/ Vendor	Website	English
Outpost24	www.outpost24.com/	Viruses	Commercial/ Vendor	Website	English
Packet Storm	http://packetstormsecurity.org/	Vulnerabilities	Commercial/ Vendor	Website	English
Pionier CERT	http://cert.pionier.gov.pl	Vulnerabilities	CERT	Website	English
PostgreSQL	http://archives.postgresql.org/pgsql-announce/	Vulnerabilities	Non-Commercial	Mailing list	English
RUS-CERT	http://cert.uni-stuttgart.de/ticker	Vulnerabilities	CERT	Website	German
SANS	www.incidents.org	Internet activity monitoring	Commercial/ Vendor	Website	English
SANS Incidents Diary	http://isc.incidents.org/	Vulnerabilities, general information, system administration	Commercial/ Vendor	Website	English
SCO	http://sco.com/support/security/2006.html	Vulnerabilities	Commercial/ Vendor	Website	English
Secunia	http://secunia.com/virus_information/	Viruses	Commercial/ Vendor	Website	English
Secunia	http://secunia.com/mailling_lists/	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Securiteam	www.securiteam.com/Mailing list.html	Vulnerabilities	Commercial/ Vendor	Mailing list	English
Security News Portal	www.securitynewsportal.com/index.shtml	Vulnerabilities	Commercial/ Vendor	Website	English
Security Tracker	www.securitytracker.com/signup/signup_now.html	Vulnerabilities	Commercial/ Vendor	Mailing list	English

Annex C: Inventory of Publicly Available Sources

Name	Weblink	Topics	Info Provider	Distribution	Language
Secuser	www.secuser.com/	Vulnerabilities	Commercial/ Vendor	Mailing list	French
SGI	www.sgi.com/support/security/wiretap.html	Vulnerabilities	Commercial/ Vendor	Mailing list	English
SI CERT	www.arnes.si/si-cert/	Vulnerabilities	CERT	Website	Slovenian
SITIC	www.sitic.se	Vulnerabilities	CERT	Website	Swedish
Sophos	www.sophos.com/security/notifications/	Viruses	Commercial/ Vendor	Mailing list	English
SQUID	www.squid-cache.org/Advisories/	Vulnerabilities	Commercial/ Vendor	Website	English
SUN	http://sunsolve.sun.com/	Vulnerabilities	Commercial/ Vendor	Website	English
Sun (blog)	http://blogs.sun.com/security	Vulnerabilities	Commercial/ Vendor	Website	English
SURFnet-CERT	http://cert.surfnet.nl	Vulnerabilities	CERT	Website	Dutch
Symantec	http://securityresponse.symantec.com/avcenter/security/SymantecAdvisories.html	Vulnerabilities	Commercial/ Vendor	Website	English
Symantec	www.symantec.com/enterprise/security_response/threatexplorer/threats.jsp	Viruses	Commercial/ Vendor	Website	English
TF-CSIRT	www.terena.nl/activities/tf-csirt/	General information	Academic	Mailing list	English
TP CERT	www.tp.pl/cert	Vulnerabilities	CERT	Website	Polish
Trend	http://uk.trendmicro-europe.com/enterprise/about_us/worldwide_select.php	Viruses	Commercial/ Vendor	Website	English
Trend Micro	www.trendmicro.com/subscriptions/default.asp	Viruses	Commercial/ Vendor	Mailing list	English
Trend Micro	www.trendmicro.com/vinfo/default.asp?advis=&sort=date&order=desc	Viruses	Commercial/ Vendor	Website	English
Trustix	www.trustix.net/errata/2006/	Vulnerabilities	Commercial/ Vendor	Website	English
Typo3	http://typo3.org/teams/security/security-bulletins/	Vulnerabilities	Commercial/ Vendor	Website	English
US-CERT	www.us-cert.gov/	Vulnerabilities	CERT Government	Website	English
US-CERT	www.us-cert.gov/current/current_activity.html	Status monitoring	CERT Government	Website	English
US-CERT Alert Tech	https://forms.us-cert.gov/maillists/	Vulnerabilities	Government	Mailing list	English
Virustotal	www.virustotal.com/en/indexf.html	Viruses	Non-Commercial	Website	English
Webmin	www.webmin.com/security.html	Vulnerabilities	Commercial/ Vendor	Website	English

Annex D: Minutes of the Meeting of the Expert Group

Meeting Minutes – EISAS validation workshop, 16.04.2007, Brussels, Belgium

Attendees:

Aarelaid, Hillar	(HA, CERT-EE, Estonia)
Andre, Gilles	(GA, CERTA, France)
Burnett, Peter	(PB, CNIP, United Kingdom)
Droz, Serge	(SD, SWITCH-CERT, Switzerland)
Huopio, Kauto	(KH, Ficora/CERT-FI, Finland)
Jedlicka, Hans Peter	(HPJ, BSI CERT-Bund, Germany)
Jochem, Aart	(AJ, GovCERT.NL, The Netherlands)
Kijewski, Piotr	(PK, NASK CERT Polska, Poland)
Leguit, Douwe	(DL, GovCERT.NL, The Netherlands)
Neves, Gustavo	(GN, CERT.PT, Portugal)
Rainys, Rytis	(RR, CERT-RRT, Lithuania)
Rohde, Martina	(MR, European Commission)
Schraml, Rudolf	(RS, Bundeskanzleramt, Austria)
Steichen, Pascal	(PS, MECE, Luxembourg)
Sturmanis, Egils	(ES, DDIRV, Latvia)
Suba, Ferenc	(FS, CERT-Hungary, Hungary)
Wallstrom, Peter	(PW, SITIC, Sweden)

ENISA representatives

Górniak, Sławomir	(SG)
Thorbruegge, Marco	(MT)

Preface and disclaimer

The following minutes are aimed to reflect the discussions that took place during the meeting. As such they are a working document that provides input for the final study report. Thoughts, scenarios etc. might not be finally phrased; open questions may still have to be discussed among the Expert Group and the other interested parties.

1. Welcome and introduction (MT/SG)

MT and SG welcomed the participants. MT gave a short overview of the EISAS request and its history (slides see Annex F). Short round of introductions. SG gave an overview of the agenda. SG defined the terms to be used during discussion for labelling information that can be shared via an EISAS:

- Static information: information with long lifespan (good practice, how-to etc.)
- Dynamic information: information with shorter lifespan (warnings, alerts and mitigations etc.)
- Real-time information: output of sensor networks (must be compiled and adapted intensively to be useful for end-users/SMEs)

2. Presentation of existing national systems (Expert Group)

Presentations from the following Member States (slides see Annex F):

- Finland (KH)
- Germany (HPJ)
- The Netherlands (DL)
- Portugal (GN)
- Austria (RS)
- Estonia (HA)
- Lithuania (RR)
- United Kingdom (PB)
- France (GA)
- Poland (PK)
- Hungary (FS)

Presentation from Non-EU Member States

- Switzerland (SD)

Annex D: Minutes of the Meeting of the Expert Group

Summary of key points to consider for the EISAS:

The presentations about national systems gave rise to some points that must also be taken into account for an EISAS:

- end-users and SMEs should be addressed in their **native language**
- the messages (warnings, good practice documents etc.) should be phrased semantically in an **understandable way** (address the non-expert)
- the manner of information dissemination should be thoroughly planned, i.e. think about other ways besides web pages and mailing lists (podcasts, RSS-feeds etc.). Make it as **convenient** as possible for the end-user/SME to obtain the information
- **avoid** information **overflow**; thoroughly plan what to publish and when to publish it
- information disseminated to end-users/SMEs must be **trusted** by the recipients for it to be accepted (on average, national governments are already trusted by end-users/SMEs)
- information should be disseminated as **close** to end-users/SMEs as possible
- **advertise** the system; an information sharing system will only be used when people know it exists
- **KPIs** are very difficult to assess; some national initiatives use questionnaires/usage studies

3. Presentation and discussion of the two inventories (SG)

SG presented the two inventories that were used to prepare the feasibility study and the validation workshop. The group agreed to consider another review and, if necessary, propose changes and additions.

4. Presentation and discussion of different scenarios (SG)

SG presented 4 different possible scenarios for an EISAS and steered the discussion. The following scenarios were presented and discussed:

Scenario 1: Europe-wide link portal

Summary: A web portal with links to existing security information

Pro: Easy and inexpensive to set up and to maintain

Con: Not much of added value

Scenario 2: Limited Europe-wide information gathering and sharing system

Summary: A system that uses the information available in the Internet and transfers it into a re-usable format that can be either picked up by end-users/SMEs or by other information sharing systems. No translation from English.

Pro: Better prepared information to be used by end-users/SMEs

Con: Only English; 'far away' from target audience (trust and acceptance)

Scenario 3: Fully fledged Europe-wide information gathering and sharing system

Summary: Independent system that uses all available sources and also produces its own information (by making use of its sensor networks, vulnerability research etc.). Translation into various languages

Pro: Native language; better prepared information to be used by end-users/SMEs

Con: Resource intensive; 'far away' from target audience (trust and acceptance)

Scenario 4: EU framework for supporting national ISASs

Summary: Expertise is gathered by the EU and brought to the Member States in the form of 'Task Forces' of experts who support the setting up of a national information sharing systems.

Pro: National/local peculiarities are considered (not 'far away' from target audience); native language

Con: Information gathering and processing will also be necessary at a national level

Discussion and results

The participants held intensive discussions on the various scenarios, which are only meant as cornerstones to mark the boundaries within which an EISAS can operate; various mixed forms or nuances are conceivable and were discussed by the participants.

Annex D: Minutes of the Meeting of the Expert Group

The following is a summary of the results of this discussion:

Systems for information gathering (and structuring) must be considered separately from a system to disseminate information to end-users/SMEs. To make the minutes more readable, 'INPUT SYSTEM' and 'OUTPUT SYSTEM' will be used in the following text to describe these two sub-systems. It must be noted that the 'INPUT SYSTEM' must also dispose of some output interfaces, through which processed information can be distributed back to the contributors (see below). The final report will include a graphical representation of the discussed idea to better illustrate the two sub-systems. The participants stress the fact that an EISAS should not compete with any national ISAS in the Member States. Additionally, an EISAS (and its sub-systems for 'INPUT' and 'OUTPUT') should provide added value not only to Member States (and their citizens) that do not have national information sharing capabilities, but also to Member States with existing initiatives.

Remarks about an INPUT SYSTEM

The INPUT SYSTEM is based on scenario 2 (see above). The target audiences for this system are the communities that contribute to it and receive 'something back' for the information that they contribute.

- a system for information gathering must be as inclusive as possible; all communities (for example, CSIRT communities, awareness-raising communities etc.) must be able to contribute to the system, but also receive benefit from the system
- the system should collaborate but not compete with existing initiatives
- added value must be provided for the various communities in order to generate incentives for contributing to the INPUT SYSTEM
- the INPUT SYSTEM must also dispose of interfaces to disseminate information back to its contributors
- the INPUT SYSTEM has to attract a high level of trust to be considered seriously
- the target group of the INPUT SYSTEM should be limited to end-users and small enterprises, as medium-size organisations should have their own administration/security team
- possible incentives for the CSIRT community might be:
 - the INPUT SYSTEM takes over some of the more 'burdensome' tasks, such as preparing ready-to-publish newsletters from contributed information
 - the INPUT SYSTEM compiles and re-structures information so that it can be easily re-used by other contributors
- incentives for other communities must be found

Remarks about an OUTPUT SYSTEM

The OUTPUT SYSTEM is based on scenario 4 (see above). It is less a system to directly disseminate information to end-users/SMEs, and more a framework to enhance the capabilities of the Member States to disseminate information to their home-users (this could even mean, when appropriate, helping a Member State to build up a governmental/national CERT to take over that task). Reason: taking into account the thoughts voiced during the presentations from the various national initiatives, it is important (for developing trust, acceptance and finally success at end-user/SME level) to carefully take into account national or even local peculiarities. Language is a crucial factor, as information has to be in the native language of the end-user/SME and must be phrased in a way an inexperienced user can understand. Additionally, information must be delivered 'as close' to the target audience as possible in order to be trusted and therefore accepted. National governments (the target group for the above mentioned framework), on average, are already trusted by citizens, and a national information sharing system (facilitated by expertise from other Member States and EU institutions such as ENISA) should build on this trust.

Remarks about both systems

When it comes to trust and acceptance, a prototype of an INPUT SYSTEM with a limited scope (concerning the type of shared information) and a small number of pilot users must prove the added value and acceptance of the pilot users. In the same way, the procedure must establish OUTPUT SYSTEMS to be piloted in a Member State in order to generate a generic case study that can be re-used on other occasions.

Systems should cover all software and operating systems used by end-users/SMEs, including the less popular ones, so they should not be limited to MS Windows and Office.

Annex D: Minutes of the Meeting of the Expert Group

5. Discussion about KPI (SG, EG)

It was agreed among the participants that it is very difficult (perhaps almost impossible) to evaluate the added value and the success of an EISAS as a whole. The most feasible scenario (including separate INPUT and OUTPUT systems) makes it a little easier to define KPIs for both sub-systems, but it still leaves considerable room for discussion about their accuracy and significance. Possible KPIs for an INPUT SYSTEM might be the number of contributing entities (CERTs, Awareness-Raising groups etc.), the amount of processed information, the number of processed information objects distributed back to the contributors and the number of connected national information sharing initiatives (that use the information but do not necessarily contribute to the INPUT SYSTEM).

Examining the success of a newly established national information sharing system (as a result of the facilitation by the OUTPUT SYSTEM) is much more complex. Some existing national activities assess their success by questionnaires or surveys. Possible KPIs could be the number of positive feedbacks from the target audience.

The assessment of the impact of an EISAS on the overall security culture in Europe was judged impossible at one precise moment of time. Assessment should be a long process.

Other KPIs will have to be discussed among the Expert Group and the other interested parties for the final report.

6. Next steps

- SG will send the inventories to the group (Expert Group and participants of the workshop) to be re-validated according to the proposed criteria and (if necessary) changed
- MT will draft the minutes and send them out to the group
- SG and MT will draft a pre-final report to be reviewed by the group
- SG and MT will further discuss KPIs, make proposals to the group and incorporate the results of the discussion into the final report
- The group (Expert Group and participants of the workshop) will review the pre-final report and the proposed KPIs and provide feedback to SG
- MT will present the final report at the security conference in Germany

Annex E: Timeline of the Study

	A	B	C	D	E	F	G	H	I	J	K	L	M
		11/2006	12/2006	01/2007	02/2007	03/2007	04/2007	05/2007	06/2007	07/2007	08/2007	09/2007	10/2007
1													
2	Phase I: Analysing current state of affair												
3	Inventory of existing ISAS												
4	ENISA own research												
5	Questionnaire NLO, PSG												
6	Inventory of sources of information												
7	Results from ENISA ad-hoc WG												
8	Own research and expertise												
9	Pre-analysis of inventories												
10	Expert group recruitment												
11	Questionnaire expert group												
12	Assessment of inventories												
13	Phase II: Examine the feasibility of an EISAS												
14	Discussion of possible scenarios												
15	Conclusion: the most feasible scenario												
16	Phase III: Assess the added value												
17	Assessing added value												
18	Discussion about indicators												
19	Recommendation of next steps												
20	Discuss recommendations												
21	Final report												
22	Draft first version of report												
23	Receive feedback from Expert group and EC												
24	Incorporate feedback												
25	Meeting with EC to discuss progress												
26	Review of second draft by Expert group												
27	Deliver final report												
28	Presentations about the study and the findings												
29	TF-CSIRT, Budapest												
30	Expert Group meeting in Brussels												
31	Security Conference in Berlin												
32	Internal ENISA presentation												
33	ITU CIIP Workshop in Geneva												

Annex F: Sample Presentation about the Feasibility Study

Examining the feasibility of an European Information Sharing and Alert System (EISAS)

ITU workshop

Geneva, 17th September 2007

www.enisa.europa.eu

Agenda

- **History of the study:** why did we do it?
- **Some definitions:** what do we mean?
- **Methodology:** how did we proceed?
- **Results:** what did we find out?
- **Next steps:** how can be followed up?
- Finalise the study

www.enisa.europa.eu

Formal Background

<http://ec.europa.eu/l2010>

http://ec.europa.eu/information_societ-y/doc/com2006251.pdf

www.enisa.europa.eu

Motivation

NIS information for citizens and SMEs is important

There is already a lot going on in the Member States, but ...

... what? ... who?

... where? ... are there gaps?

... how? ... where are the gaps?

And finally: what can the EU do?

www.enisa.europa.eu

Objectives

- **Goal:** raising awareness on NIS issues
- **Target group:** citizens and SMEs
- **Base:** existing systems

Terms & Definitions

- Feasibility Study(!)
- Information Sharing & Alerting(?)
- NIS Security related Information (Good Practice & Recent Developments)

www.enisa.europa.eu

Methodology of the study

- **Analyse** the current “state of affairs”
- **Develop** possible scenario(s)
- **Determine** the most feasible scenario
- **Determine** the added value

Start: 09/2006
End: 10/2007

www.enisa.europa.eu

Support by a group of Experts

- Nominated by the EU Member States (NLO network) and the Permanent Stakeholder Group (PSG)
- Expertise in running Information Sharing Systems
- Contribute to the study

➔ 15 Experts from the Member States & Switzerland

www.enisa.europa.eu

Analyse the current “state of affairs” (I)

13 Annex B – Inventory of existing systems

System Name	Usage	Operator	System Type	Notes
ENISA IT
...
...
...
...
...
...
...
...
...
...
...
...
...

www.enisa.europa.eu

Annex F: Sample Presentation about the Feasibility Study

But: Following the analysis (I) EISAS should provide

Added value by collecting and sharing good practice

to support national systems!

www.enisa.europa.eu 17

Following the analysis (II) EISAS should provide

Added value by fostering dialogue

among the Member States and existing initiatives

www.enisa.europa.eu 18

Following the analysis (III) EISAS should provide

Added value by encouraging synergies

for example to avoid double work

www.enisa.europa.eu 19

Proposal for next steps

Discussion involving all stakeholders, ...

... involving the Member States, ...

... involve European experts and ...

Added value by collecting and sharing good practice

... further develop scenarios and initiate a proof of concept.

www.enisa.europa.eu 20

Finalise the study

Planned end of October 2007

www.enisa.europa.eu 21

Questions, comments, compliments, threats?

EISAS@enisa.europa.eu

www.enisa.europa.eu 22

Alerts & Warnings

Information about NIS threats, disseminated by all possible means. Usually alerts & warnings must be accompanied by recommended actions the user should take to mitigate a threat arising on the Internet.

CERT (Computer Emergency Response Team)

An organisation that studies computer and network security in order to provide incident response services to victims of attacks, to publish alerts concerning vulnerabilities and threats and to offer other information to help improve computer and network security.

CSIRT (Computer Security and Incident Response Team)

Another term for CERT.

Culture of security

Awareness about NIS-related matters and the corresponding behaviour of Internet users, defined by the OECD guidelines "Towards a culture of Security"¹³.

EISAS (European Information Sharing and Alert System)

The subject of this study; a placeholder for a yet-to-be determined role that the European Union can take in the area of sharing NIS information with citizens and SMEs. Describes a concept, not necessarily a physical system.

Good practices

Ways of reacting to NIS threats that have shown their usefulness in the past and are currently used with success by many people.

Hacker

A person who studies and explores software and systems with the aim of finding the weaknesses and vulnerabilities that allow him/her to break into remote computers.

Home-users

In the context of this study, a generic group of people who use the Internet at home, as a tool, without deep knowledge about how it works.

Information dissemination system

A logical part of the EISAS; a subsystem disseminating information to end-users.

(N)ISAS

In general, an information sharing and alert system; facilities providing information to its users. Within this study this term is used to describe existing (national) information sharing activities.

(EU) Member State

A state belonging to the European Union.

NIS

Abbreviation for Network and Information Security.

NLO (National Liaison Officer)

ENISA's primary contact point with a Member State¹⁴.

PSG (Permanent Stakeholders' Group)

An ENISA body; a group composed of experts representing the relevant stakeholders, such as the Information and Communication Technologies industry, consumer groups and academic experts in network and information security. The Permanent Stakeholders' Group advises on the drawing up of the Agency's work programme and in ensuring communication with the relevant stakeholders on all issues related to the work programme¹⁵.

¹³ OECD guidelines - www.oecd.org/document/42/0,2340,en_21571361_36139259_15582250_1_1_1_1,00.html

¹⁴ ENISA NLO Network - www.enisa.europa.eu/pages/03_02_01.htm

¹⁵ ENISA PSG - www.enisa.europa.eu/pages/03_03.htm

Annex G: Terms and Definitions

Real-time information

In the context of this study, describes information concerning the actual state of the network, gathered through sensor networks.

RSS-feed

A method of information dissemination via dynamic web content. The meaning of the letters RSS has changed over time (from 'Rich/RDF Site Summary' to 'Really Simple Syndication').

Sensor network

A system using sensors to gather overall information about the current state of the network. A sensor is usually a computer system or a packet routing device connected to a network that collects information about data traffic in the segment to which it is connected.

SME

Small (fewer than 50 employees) and Medium (fewer than 250 employees) Enterprises. The numbers vary in the various Member States. A more precise term would be 'Micro Businesses'.

Source of information

In the context of this study, a web portal, mailing list or some other system that is capable of providing NIS-related information, and is publicly available.

Virus

Malicious code that might replicate itself and infects other computers with the help of a user (i.e. opening an e-mail or an attachment).

Vulnerability

Weakness in software or hardware or its configuration that may lead to a break-in or otherwise compromise the security of a system.

Worm

Malicious code that replicates itself and infects other computers without the interaction of a user.

XML (Extensible Markup Language)

A data format widely used to facilitate the sharing of different types of data.

Authors:

Marco Thorbruegge, Senior Expert in Computer Security and Incident Response, ENISA
Sławomir Górniak, Seconded National Expert

For further information about this report:
CERT-Relations@enisa.europa.eu

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.

© ENISA – European Network and Information Security Agency, 2007



ENISA - European Network and Information Security Agency
PO Box 1309, 710 01, Heraklion, Crete, Greece
Tel: +30 2810 39 12 80, Fax: +30 2801 39 14 10
www.enisa.europa.eu