Good Practice Guide

Network Security Information Exchanges

enisa
European Network and Information Security Agency

Acknowledgements

About ENISA

This report was prepared by Symantec Inc. in co-operation with Landitd Ltd. on behalf of ENISA.

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

This report is based on the responses given by experts coming from several member states. ENISA would like to thank all these countries for their contribution, namely: UK, NL, SE, DE, NO and CH.

ENISA would also like to thank Symantec Inc. in co-operation with Landitd Ltd for their professionalism and dedication that resulted in this great report.

Contact details

More information on this report or ENISA's activities on the resilience of public eCommunications Networks can be obtained by

Dr. Vangelis Ouzounis
Senior Expert, Network Security Policies
Technical Department
ENISA
Email: resilience@enisa.europa.eu, Web: http://www.enisa.europa.eu/resilience

Table of contents

Executive Summary

Information sharing among private and public stakeholder is a powerful mechanism to better understand a constantly changing environment and learn in a holistic way about serious risks, vulnerabilities and threats, as well as solutions.

The European Commission assessed first the opportunity of developing the first pan European Information Sharing and Alerting System (EISAS[1]). ENISA was called for to define the requirements of such a pan European system.

ENISA's stock taking and analysis[2] on this topic confirmed the importance and strategic value of information sharing. The recent EU Commission Communication on CIIP[3] identified information sharing as a strategic area for Europe and called for additional action.

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

An Information Exchange is a form of strategic partnership among key public and private stakeholders. In the NIS field, these can sometimes be referred to as 'Network Security Information Exchanges' (NSIEs) although it is recognised that alternative names can also be used.

The scope of this partnership is limited to addressing the security and resilience of eCommunication networks that carry voice and data services over the fixed and mobile (wireless) infrastructure in both the public and private circuit domains.

The partnership works by exchanging information on cyber attacks, disaster recovery or physical attacks. The drivers for this information exchange are the benefits of members working together on common problems and gaining access to information which is not available from any other source, but only from competitors and national security agencies.

Through sharing of experience and sensitive information the groups develops jointly recommendations for mitigating risks and threats and continuously assess existing measures in light of new

[1] http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf

[2] http://www.enisa.europa.eu/pages/resilience.htm#analysis

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

developments. The platform could also provide unique strategic insights to policy makers and strategists about emerging policy issues.

Today, unfortunately, there are only a few Member States in Europe actively running NSIEs.

The main aim of this guide is to assist Member States and other relevant stakeholders in setting up and running NSIEs in their own countries. Hopefully the guide will pave the way for an accelerated deployment of national NSIE and consequently co-operation among public and private stakeholders at pan European level.

This guide is based on an analysis of different information from a number of sources, including the results of a questionnaire sent to a number of European countries, desk top research on a number of non EU countries that demonstrated expertise and knowledge in the area and individual discussions with expert. The content of this Guide represents the aggregation of good practice from a number of countries.

Introduction

Policy Context

Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures.

They are typically regarded as critical information infrastructures (CIIs)[4] as their disruption or destruction would have a serious impact on vital societal functions.

In 2005, the Commission[5] highlighted the urgent need to coordinate efforts to build trust and confidence of stakeholders in electronic communications and services. A strategy for a secure information society[6] was adopted in 2006. Its main elements, including the security and resilience of ICT infrastructures, were endorsed in Council Resolution 2007/068/01.

On the regulatory side, the Commission proposal to reform the Regulatory Framework for electronic communications networks and services[7] contains new provisions on security and integrity, in particular to strengthen operators' obligations to ensure that appropriate measures are taken to meet identified risks, guarantee the continuity of supply of services and notify security breaches.[8] This approach is conducive to the general objective of enhancing the security and resilience of CIIs. The European Parliament and the Council broadly support these provisions.

A key element of European Commission strategy in this area is the European Programme for Critical Infrastructure Protection (EPCIP)[9]. Important elements of this program were the Directive[10] on the

[4] *A definition of CIIs was proposed in COM(2005) 576 final*

[5] *COM(2005) 229*

[6] *COM(2006) 251*

[7] *COM(2007) 697, COM(2007) 698, COM(2007) 699*

[8] *Art. 13 Framework Directive*

[9] *COM(2006) 786 final*

[10] *2008/114/EC*

identification and designation of European Critical Infrastructures[11] and the Critical Infrastructure Warning Information Network (CIWIN)[12].

In the context of this program European Commission supported the pilot development and deployment of EISAS, the European Information Sharing and Alerting System. EISAS is about reaching out and alerting citizens and SMEs based on national and private sector information. The Commission financially supports two complementary prototyping projects.[13] ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS.

In 2008 ENISA in co-operation with the Commission and the Member States recognised the importance of Resilience of public Communications Networks and developed a Multi-annual Thematic Program (MTP).

ENISA's Resilience Program on the resilience of public e-Communication networks performed stock taking and analysis of Member States' (MS) policy and regulatory environments. The analysis of the stock taking findings revealed the importance of good practices in numerous areas including information sharing exchanges.

Information Exchanges is an under explored concept in Europe, as well as other parts of the world but countries that have long experience in this area strongly recommend the establishment of such a strategic public private partnership with major stakeholders.

ENISA's stock taking and analysis[14] on this topic confirmed the importance and strategic value of information exchanges. Member States are strongly interested in better understanding and deploying the concept of NSIE and requested ENISA to develop a good practice guide based on observed practices of existing exchanges.

Risks, vulnerabilities and threats are global. Actually sharing of information at national level does not fully address the problem. As Member States develop effective information exchanges at national level they pave the way for wider collaboration and deployment at pan European level. ENISA role in such a

[11] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf

[12] *COM(2008) 676 final*

[13] *Under the EC Programme "Prevention, Preparedness and Consequence Management of terrorism and other Security Related Risks"* http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

[14] http://www.enisa.europa.eu/pages/resilience.htm#analysis

case would be instrumental in developing further the concept and bringing all these stakeholders at pan European level.

Scope

An Information Exchange is a form of partnership among public and private stakeholders involved in the provision of telecommunications services and networks. Its scope is limited to addressing the security and resilience of eCommunication networks that carry voice and data services over the fixed and mobile (wireless) infrastructure in both the public and private circuit domains.

The partnership works at a tactical and strategic level by exchanging information on security incidents, vulnerabilities, threats and solutions in a trusted environment to ensure that barriers to sharing are minimised.

The focus of this exchange is mostly to address malicious cyber attacks, but also natural disasters or physical attacks. The drivers for this information exchange are the benefits of members working together on common problems and gaining access to information which is not available from any other source, namely competitors and national security agencies.

[Switzerland] *'membership allows for the National Critical Infrastructure to get their hands on additional expertise and information to support their information security process, which they would not have access to otherwise.'*

A common name for this public/private sector partnership is a Network Security Information Exchange (NSIE) which for simplicity is the name used within this Guide although it is recognised some member states use alternative names.

Target audience

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

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

These operators and users are likely to be involved in Critical Information Infrastructure Protection (CIIP) and have an interest in both public and private networks and the services which they support.

Aims of the Guide

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

A longer term aim is for the Guide to support the development of common approaches and policies for information exchange so as to facilitate working relationships and understanding between each country's NSIEs.

The approach adopted within the Guide is based on providing a choice. This choice is based on an understanding of observed good practice which the reader can follow, or not, depending on its relevance to their own country's eCommunications environment.

Structure of the guide and how to use it

The structure and content of this Guide has been created from an analysis of research into current good practice among existing NSIEs, using the results of a questionnaire (Appendix B), desk research and advice from experts on the subject. This analysis looked at the Why, What, How and Who in relation to setting up and running an NSIE, as well as capturing the aspirations of what ENISA would like to see in the future.

Within the guide, issues and good practices are described within the various sections, using short quotes, presented in italics, from various sources to validate the points being made. At suitable stages, observed good practices are highlighted to aid the reader of the guide make a choice whether the observed good practice is relevant to their own environment and need. These observed good practices are presented in a text box.

Each section of the report is summarised below:

Section 1 'Introduction' (above) has explained the scope of this Guide, its aims, its target audience, and how the rest of the Guide is set out. It also describes definitions and abbreviations.

Section 2 'Preparation and Planning' describes what an NSIE looks like, with statements on its characteristics - what it does, how it behaves, its expectations etc. These are the characteristics based on good practice observed in existing NSIEs so the reader can start to visualise an NSIE as an entity.

Section 3 'Organisational Structure and Membership' then looks at the operational aspects , starting from the first Information Exchange meeting and addressing issues such as what type of information is

exchanged, how the information can be exchanged and who is allowed to see it. Ongoing governance and relationships with other bodies is also addressed.

Section 4 'Actions to Set up an NSIE' ; this section is much more directed, giving practical strategies to adopt when you decide to set up your own NSIE. We take you through the groundwork needed before the NSIE begins, the initiation stage, and outline many of the operational procedures we have observed when looking at established NSIEs.

Section 5 'Evolution and vision' concludes the Guide by providing hopes for the ways in which this document might support further developments in those countries who are aware of the benefits which an NSIE can offer, and aspirations of ENISA for the future development of NSIEs. Useful references are detailed in Appendix A.

Definitions

For the purposes of this document, the following terms and definitions apply:

CSIRT (Computer Security and Incident Response Team):

An organization that provides incident response services to victims of attacks, including preventive services (i.e. alerting or advisory services on security management). The term includes governmental organizations, academic institutions or other private body with incident response capabilities.

Critical Information Infrastructure: Those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy. [Source: OECD 2008]

Electronic communications (eCommunications) Networks: Transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, radio, optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. [Source: EU Directive 2002/21/EC].

Network and Information Security (NIS) The ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems. [Source: ENISA]

Public communications networks: electronic communications networks used wholly or mainly for the provision of publicly available electronic communications services; [Source: EU Directive 2002/21]

Private communications network: Any network used to communicate within an organization (as distinct from providing service to the public) or to supply such communications to organizations, based on a configuration of own or leased facilities. The term includes networks used by private companies, state enterprises, or government entities. [Source OECD: http://stats.oecd.org/glossary/detail.asp?ID=4961]

Resilience: The ability of a system to provide & maintain an acceptable level of service, in face of faults (unintentional, intentional, or naturally caused) affecting normal operation. [Source: ENISA]

Abbreviations

For the purposes of this document, the following abbreviations apply:

CERT	Computer Emergency Response Team
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
CNI	Critical National Infrastructure
CPNI	Centre for the Protection of National Infrastructure (UK)
DPA	Data Protection Act
FOIA	Freedom of Information Act
NCO-T	National Continuity Forum Telecommunications (NL)
NDA	Non Disclosure Agreement
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee (US)
TLP	Traffic Light Protocol

Preparation and planning

Overview of NSIEs

Before looking in detail at good practice for setting up and running an NSIE, it is useful to look at the overall concept. At a high level, several NSIEs have drawn up mission statements with a view to specifying clearly and succinctly what the NSIE is and what it aspires to be.

It is a good idea to involve as many stakeholders as possible in producing and refining the mission statement, and this helps develop a sense of ownership and responsibility.

Here are two examples:

[USA]

The NSIEs share information with the objectives of:

- Learning more about intrusions into and vulnerabilities affecting the Public Network
- Developing recommendations for reducing network security vulnerabilities
- Assessing network risks affecting network assurance
- Acquiring threat and threat mitigation information
- Providing expertise to the NSTAC on which to base network security

[Netherlands]

Within the group, the government, together with the providers, seeks to:

- create preventive measures to prevent serious disruption or failure of public communications networks and services,
- take measures to rectify any disruption or failure as soon as possible and with as little damage to critical interests as possible.

Observed characteristics of an NSIE

When you consider setting up an NSIE, it helps to understand what the final entity will be and how it will operate. For those new to NSIEs, this section describes what an NSIE looks like in terms of its characteristics and features based on observed examples of NSIEs.

NSIEs address strategic and tactical issues

The emphasis is on major disruption. Information exchanges are concerned to protect against attack and to acquire early evidence of its likelihood, rather than in damage recovery. Specifically NSIEs employ the members' technical expertise and operational capability to:

- identify emerging threats and analyze their potential impact on communications networks and information systems
- assess the impact of incidents (security breaches, network failures, service interruptions)
- identify, analyse, and adopt appropriate coordinated preparedness measures to mitigate such threats and risks
- set up internal and joint procedures to continually review the implementation of adopted measures

NSIEs usually do not have an operational role or respond to crisis

NSIEs usually do not have an operational role or respond to crisis. In some instances, where trust among participants is high, members could provide mutual assistance to their peers and strategic advice to public participants.

NSIEs focus on electronic/physical attacks, malfunctions of systems, interdependencies with other sectors and natural disasters

The major focus of NSIEs is on threats related to electronic/physical attacks but also malfunction of systems, interdependencies among sectors and natural disasters. The consequences of such threats might result in physical damage (e.g. failure of reservoir telemetry, electricity supply failure). Furthermore, physical attacks targeting telecommunications infrastructure (e.g. cable-based networks) may result in emergency procedures such as unencrypted wireless bypass, with known security weakness. Consequently, NSIEs exchange information with other CIP bodies.

NSIEs provide commercial benefits to its members

eCommunication providers report a number of commercial benefits from taking part in an NSIE. There is an operational benefit from cost-savings and time to react to (or even to anticipate) serious network failures, and there are possibilities to influence government policy and avoid the introduction of misplaced regulation. There are other directly commercial benefits, for example:

[UK] *'After we (major telco) detected and fixed a potential weakness in our own network, we realised that we could not make a commercially valuable interconnection to a number of correspondent providers without sharing our findings.'*

NSIEs place emphasis on information exchange, not information transfer

NSIEs are peer-to-peer organisations, with flows of information that are balanced in terms of giving and receiving. All members actively share as well as listening. In this regard, they can be distinguished from CERTs/CSIRTs, which tend to issue greater quantities of authoritative information than they receive.

NSIEs recognise that their members have commercial sensitivities

Quality of service is commercially sensitive between competitors, which presents a barrier to sharing. Network providers are reluctant to reveal too many details regarding weaknesses and vulnerabilities to customers as it could affect their market standing. Also, if they reveal problems to the regulator, it might have to enforce regulations.

NSIEs choose their members carefully to remove barriers to sharing

Although network providers compete with each other, they can see advantages working together in dealing with equipment vendors and suppliers. They may not want the suppliers to be directly part of the Information Exchange because of the risk that sensitive information will be used for commercial advantage but an NSIE can create mechanisms for controlled interaction when needed.

NSIEs see Government as having a key role in its creation and operation

The government members may belong to a variety of organisations within government, but it is usual for leading government administration to report into a civilian rather than military body. Examples observed included telecommunications and industry ministries, as well as those associated with internal security.

The role of government as honest broker with no commercial interests and also as the provider of threat information which is not available else where, is one of the critical success factors of an NSIE.

NSIEs are generally quite small organisations

Several organizations told us that that it is important to *'start small, and only increase membership if necessary.'* This was seen as having several benefits: minimizing cost and agenda administration, allowing time to gain experience in running the NSIE and, perhaps most important, ease of building trust.

NSIEs are designed to encourage mutual trust

Members are expected to give the same level of information as they receive, under conditions of confidentiality. Keeping membership small fosters trust. The core of the Information Exchange is a set of regular face-to-face meetings.

NSIEs members are senior executives with relevant skills

NSIE members are senior experts that have management authority to share sensitive information with their peers. They normally have a strong background in security and resilience and could mobilise resources wherever change is needed to address vulnerabilities, risks and threats (Chief Security officer or equivalent).

Meet regularly, face-face, to share sensitive information

The members of an NSIE meet regularly and face-to-face (usually 4-6 times per year) to share information. Sharing of sensitive information is done using standard mechanisms (e.g. Traffic Light Protocol). Disseminate of information could also be done through protected extranets usually managed by the government. As trust within the group grows, members develop informal links via telephone and/or email.

No participation fees for members

Usually there are no participation fees. The costs of running the NSIE are usually covered by the government. Stakeholders taking part in an NSIE consider it cost effective but a participation fee could be seen as a barrier, especially during the early life of an NSIE..

Twin chairs, one from industry and one from government

Usually NSIEs are chaired by two chairs, one coming from the public and another from the private stakeholders. Alternatively, the chair of the NSIE could rotate between private and public sector on a regular basis.

The role of the chair(s) is in setting the agenda, organising the events and managing the discussions.

New members require unanimous agreement of existing members

Usually participation of new members in the NSIE requires the unanimous agreement of existing members. This is extremely important as new members can disturb the existing trust among participants.

NSIEs recognise that incentives are needed for members to participate

Most NSIE members see clear benefit in taking part as they receive valuable information from government, and from their sector colleagues. Governments in particular recognise the value of their information as an incentive to encourage others to share information and consequently put significant effort into ensuring its quality and timeliness.

NSIEs are often set up after a security 'scare'

We found that NSIEs were often set up after a major incident provided evidence that an NSIE organisation was needed, or after a country became aware of 'worst case scenarios'.

[UK] *'We (major telco) had been pestering management for some time over emerging risks without success. Then Government started to look seriously at the cyber threats and formed a committee where they needed the carriers on board but lacked strong connections. Around then we discovered a critical problem that required collaboration with other major carriers. Knowing of an existing NSIE example, and with the help of Government, we were able to explain the seriousness of the matter and the benefits of the secure information exchange model. Perseverance, a precisely described and critical example and help from Government, were key ingredients.'*

Organisational Structure and Membership

With an understanding of the characteristics of an NSIE and an understanding of the environment in which it will operate, we can now consider the specific elements of an NSIE.

NSIE membership

All participants share information in a two way exchange between industry and government and industry and industry. To reflect this, most existing NSIEs are jointly chaired by a representative from government and from industry.

Central to the effective working of the NSIE are regular, face-to-face meetings which establish trust and facilitate a free exchange of ideas. As and when decided by the members, other attendees may be permitted to attend if they have useful information they can share.

The NSIE can create sub-groups and working groups, to take forward detailed work projects and appropriate members can be invited to join.

There are clear rules and guidelines covering conduct and membership of an NSIE.

The important characteristic of members is that they are empowered to speak on behalf of the organisation they belong to. Members do not necessarily need in-depth knowledge of security technology but they must be empowered to direct that security enhancements take place in their organisation. In most cases each organisation can put forward a maximum of two representatives. When a company sends two representatives, it is common for one to cover policy, and one to have operational, technical experience.

[UK] *'Generally members will be security or risk managers. Many members will have specific information security roles. Members are usually chief or deputy information security officers and must be conversant with telecoms and information security issues.'*

Members must not only have the right knowledge but must be empowered and willing to share as well as attend meetings regularly for continuity.

Exchange of information in an NSIE is based upon the personal trust of representatives, sharing information in a confidential meeting. Representatives are expected to attend all meetings so that face-to-face, they build up a trusted community. Members must be active, in at least providing to each meeting a short report on issues affecting their parent organisation.

According to the majority of answers received, a member organisation may be asked to leave the exchange if neither of its representatives attends three successive meetings.

NSIE member organizations are required to sign an NDA and all representatives must have security clearances appropriate to their country. See example in Appendix E

[Switzerland] *– 'Members sign a Non Disclosure Agreement, which has to be adhered to. Breaking the rules of conduct or other rules stipulated in the NDA will result in actions which, can lead to being excluded from the Information Exchange.'*

There should be clear agreed rules and guidelines for the organisation and structural workings of an NSIE. This would normally include an NDA.

Building trust in an NSIE

An NSIE must consider the question of trust seriously as it will only succeed if members feel able to trust each other. When you share information, particularly that whose unauthorised leakage might damage your organisation, you take a risk. Trust and value grow together but need investment. If trust is broken it is slow and difficult to rebuild. With maturity of trust comes greater value as the higher the trust, the more people feel able to share.

Trust is personal – it grows slowly between people. Therefore meetings take place face-to-face, and representatives must attend. They cannot send a substitute as a stranger turning up at a meeting would inhibit the sharing of sensitive information.

It is important to establish, and consistently use, codes of practice that minimise the risk of breaches of confidentiality, and increase trust. NDA's and different levels of information sharing provide members some protection from unauthorized disclosure.

An agreed distribution policy has been shown to help build trust. The Traffic Light Protocol was found to be used widely where Red information is the most sensitive. Other good practice used by some NSIEs is the 'Chatham House Rule'. See Appendix C and D for TLP and 'Chatham House Rule'.

[Netherlands] *'if designating a distribution policy doesn't happen, and there is a subsequent doubt about what information can be used and what can't , the default position for many will be to not use the information i.e. treat it as RED. Consequently it will be buried and any benefits from sharing it will be lost.'*

When sharing information, the owner of the information should always state the dissemination rules for that piece of information. If the whole meeting is designated AMBER, everyone should know this from the start, and feel able to trust the group to handle it accordingly. Additionally, and vitally for information sharing, they should be encouraged to share more sensitive (more critical) information by declaring, for example, that it is RED

Some of the information shared inside an NSIE will have a degree of sensitivity attached to it. In order to protect national security interests the Government agency involved carries out security checks on the company and the individuals as well as checks against official records.

Professional competence enhances trust. If a company adopts widely accepted accredited procedures such as ISO 9001 (Quality Management) and ISO 27000 (Information Security) this helps an organisation to become trusted.

An NSIE must recognise and manage the potential threats to company interests and thus to trust. Such things as regulatory action or suggesting prosecution do not promote trust. This is why the position of the Regulator must be carefully considered.

[UK] *'The key to the success of information exchanges is trust. Identity and employment verification checks are performed on all applicants as well as checks against official records. Information is shared under the Traffic Light Protocol (TLP).'*

[Netherlands] *'Building trust to get competitive providers talking with each other on sensitive (possibly company confidential) items (was a difficulty we encountered) Success because the government started with bilateral talks on the subject and showed that it was ensured that company info was kept confidential.'*

One key to an NSIE's success is trust. Building up trust is seen as a priority. This would be supported by NDAs and procedures for sharing information securely.

Focus on relevant value add services

It may sound obvious that the information exchanged must be relevant to the NSIE members and add value, but observations have been made where information has been introduced which has little value. This can easily happen when the threat is low with few incidents to discuss but it is thought better to have shorter meetings than fill the meeting with low value information. To prevent this happening it is good practice for the NSIE to state clearly the scope and criteria of the services it provides.

[Switzerland] *'services offer everything from security advisories to warnings and best practices. However, such information must pass the following criteria:*

1. *It must concern and support a member, the whole sector or all parties in their mission to strengthen their information security process.*
2. *The information must have an added value. (i.e. not available somewhere else).'*

Another key to NSIE's success is to focus on exchanging relevant information which adds value to members and is not easily available elsewhere.

Interfaces with an NSIE

An NSIE must have relationships with government and others. This section describes an NSIE's position with regard to other organisations concerned with network security, national regulation, and international interests in both public and private sectors.

Relationship with Law Enforcement

Reporting into or engaging permanently law enforcement agencies has been specifically avoided in some countries:

[UK] *'The Police/Regulators had statutory duties to report certain types of activity, which may conflict with the aims and wishes of the group, and notably with the IE's confidentiality agreement.'*

[New Zealand] *'Overseas experience shows that the center should not be part of a law-enforcement agency, since this might reasonably focus on the pursuit of offenders, to the detriment of rectifying damage and of confidentiality'*

Advice should be sought at an early stage about the role of law enforcement on whether they would be able to agree to the NSIE rules on disclosure.

Relationship with Telecommunications Regulator

The relationship with any Telecommunications Regulator might be problematic. There are several reports of the reluctance of the industry members to talk freely in forums that are too closely connected with the telecommunications regulator. One source reported that the NSIE failed because of Regulator's presence.

Against this, there are occasions where Information Exchange members have welcomed the opportunity to hear the views of the Regulator on issues that might impact on NSIE activities and, in these cases, it has been considered appropriate for Regulators to attend, selectively, as an invited member. Indeed, one government coordinator told us that:

[Switzerland] *'The regulators are not members, however, especially in the sector of telecommunication there is a well established contact to the telco regulator. If the sectors or members wish, the regulator is invited to look at certain problem fields. However, the regulator is in no shape or form affiliated.'*

[UK] *Where there is a difference of views between the Regulator and the network providers, it usually turns out that the views of the government members tend to agree with the industry members rather than the Regulator.'*

Careful consideration should be given to how the Telecommunications Regulator should or should not be directly involved in the NSIE, depending on the regulatory environment and members views.

Relationship with CERTs/CSIRTs

NSIEs usually do not engage directly on a regular basis technical experts from national or governmental CERTs. In some cases, experts from national CERTs/CSIRTs are engaged in the analysis of a particular vulnerability, risk or threat.

Although both CERT/CSIRT and an NSIE are concerned with network security, they are quite different with different roles and functions, different people, and a different purpose.

CERTs, or CSIRTs as they are often called in Europe, are organizations usually providing incident response services. They have an operational character (response and restoration) and specific scope in dealing with real time issues. Recently CERTs/CSIRTs also address prevention issues though at different level of abstraction as NSIEs. In CERTs/CSIRTs the information flow is generally from the CERT/CSIRT to its members.

NSIE, on the contrary, have a wider focus on planning, prevention and supply chain issues. They are addressing the bigger picture for the general good of the industry. NSIEs usually do not have operational character nor respond to crisis. The focus of an NSIE is on protection and deterrence, usually with a post-event time frame. The members, from public bodies and private organisations, share information in an equal, two way flow, each learning from each other.

A national CERT/CSIRT has a closed community of government departments and can use enforceable protectively marked vetting procedures to build trust. A private sector CERT/CSIRT within a company is again a closed community of employees where they can use policies and employment contracts to help build trust.

NSIEs members' are commercial competing companies, sharing information between themselves and government security agencies. An NSIE must therefore spend a significant amount of effort on building and maintaining trust to enable the public and private stakeholders to cooperate.

Careful consideration should be given to whether or not and how experts from national CERTs/CSIRTs take part in NSIEs.

Relationships with other Resilience-related bodies

NSIEs take note of relevant good-practice processes originated elsewhere, as well as making appropriate contributions to the development of more general resilience good-practice. However, it is not usual for the NSIE to communicate directly and fully with other resilience or CIP bodies; it is generally the case that all interaction is via the government representative on the NSIE who deals with these organizations, and who can appropriately sanitize the information that is passed.

Each country has to adapt an NSIE to its own unique political, cultural and economic circumstances. Where information exchange is planned across a number of countries, care must be taken to adopt policies appropriate for all members.

Funding and costs

Government and industry pool their information and learn from each other where participation in an NSIE can increase operational efficiency, increase productivity and effectiveness, and decrease costs.

In the NSIEs studied, central funding is provided from the government for secretariat and all administration, including web-portal management if this is used. Generally, the host Government organisation provides the venue and lunch, although some NSIEs occasionally meet at a member's organisation.

[Netherlands] *'During the start-up phase of the info-exchange all costs were paid for by government. (costs for: meetings, consulting independent experts, independent chair of the project team during startup phase, brochures).'*

Membership of an NSIE should be free at the point of delivery, with the only cost to members being their time and travel expenses.

Legal considerations

There are a number of legal implications relating to creating and setting up a Public/Private Partnership NSIE which are likely to be different in each country, depending on the legislative environment. For example, some countries such as England have a common law environment where the interpretation of legislation is determined by case law, whereas some Scandinavian countries have a civil law environment where the legislation can be interpreted as soon as legislation is enacted. This has implications for NSIEs in relation to, for example, the Data Protection Act (DPA) and Freedom of Information Act (FOIA) which can be more of a barrier to sharing in some countries than others.

There are also legal implications with anti-competitive aspects of sharing with a limited number of industry experts. The following are some legal aspects to consider:

Cartel: It is important to ensure the group is not open to accusations of becoming a cartel (there are specific actions in some countries that are illegal): a possible solution is to enforce a policy of not discussing the commercial aspects of any individual product or service.

Commercial Advantage: In an industry containing many hundreds of service providers how do you share information with a few of them without giving them a commercial advantage? There is a need to share in a trusted environment and this trust can only be formed in small groups (studies show that the most effective size of a sharing, trusting group is between 20 and 30, no more) but it is important for the trust to be complete i.e. to trust industry and every industry member had to trust the rest. Every effort must be made to ensure that the companies providing the critical infrastructure are represented, and that they (the company) selected the individual to work with. It is also important to take steps to make the shared information available to the rest of the industry through, for example a public website.

NDA: Some NSIEs initially determined that a legally binding non-disclosure agreement may make sharing difficult and so developed a set of non-binding sharing guidelines. This was shown to change over time when a partner NSIE (under a different legal jurisdiction) insisted on a legal NDA to provide enhanced access to a specific website; to facilitate this the group developed a legally binding NDA between members that contained the same conditions as the NDA of the partner NSIE.

OSA and FOIA: Some NSIEs are in a unique situation in that all information sharing is covered by the National Security legislation such as the Official Secrets Act of UK. This can make sharing easier, once the members are aware of the national security aspects of the work. Similarly, there is an option to exempt some advice from disclosure under the Freedom of Information Act (FOIA) in the interests of national security, if applicable.

Limit of liability: It is important to caveat advice with a limited liability; we are not liable for any actions carried out by the members based upon any information shared.

[The CIIP Survey, Vol 2] *'Members are afraid to divulge information because of worries about liability due to risk of antitrust violations, and the loss of proprietary information. As a first step, information sharing requires a permissible legal framework.*

Legal advice should be sought when creating an NSIE to ensure that it will operate in a permissible legal framework.

Information inputs and outputs

What information is shared?

Information that might usefully be shared in NSIEs would include: incidents, product technical vulnerabilities and risks, protocol vulnerabilities, network intrusion information, probing attacks and network configuration issues within standards.

To maintain trust NSIEs need to be very sensitive in approaching commercially sensitive issues such as quality of service and availability, which are seen by some private sector members as having significant competitive advantage. Forcing detailed disclosure of such information, for instance, could seriously damage relationships, and in some countries may be considered illegal if industry members could be considered setting up a cartel.

The following descriptions of what is shared have been observed:

- Sharing experience on threats, attacks, counter measures, response, cooperation, etc;
- Advisory support in implementing protective measures;
- Alert service on attacks and incidents;
- Information on cyber security, analysis on threats, risks, impact and vulnerabilities, incidents, security measures, etc;
- Information on contingency planning, analysis on threats, risks, impact and vulnerabilities, on single point of failures, dependencies, crisis management arrangements, incidents, exercises, etc;
- Everything from security advisories to warnings and best practices;
- Any type of information which is deemed interesting and valuable in order to support increasing the NSIE members information security, is collected, disseminated and shared;
- Peer good practice;
- Incidents and vulnerabilities and also discussions around good practices and recent trends and developments;
- Information, physical and personnel security information is collected from a wide range of sources.

How is information shared and validated?

The following are examples of how the information is shared, exchanged and validated:
The primary method of sharing is face to face in the NSIE meetings;

Protocols for distribution such as the TLP help build trust;

Some NSIEs use a protected extranet for announcements, meeting summaries and action items.

[UK] *'NSIE members have access to the government's extranet portal, which provided a need-to-know set of web pages for NSIE only and a range of documents of general interest that are not issued publicly.'*

The website is normally managed by the government host

Vulnerabilities are analysed through risk/threat/impact analysis. The outcome of this analysis is the basis for the decision if measures are needed, and if so, what measures;

As trust within the group grows, members develop informal links via telephone and email;

When a network of trust has been established, an NSIE will sometimes organise conference calls to provide immediate assistance to NSIE member organizations when urgent security concerns arise.

[US] *- 'Although most often NSIE representatives share their information at the bimonthly meetings, events occur that warrant a more rapid response and representatives communicate with each other on an ad hoc basis between meetings. Through personal contacts, telephone, and e-mail, NSIE representatives have developed an informal, accelerated information sharing capability. Such event driven communication allows Government and industry representatives to collaborate to rapidly contain, respond to, and recover from an incident, mitigating the impact of the incident. In addition, relationships with NSIE representatives provide Government with industry POCs to confirm events in real-time.'*

Create a variety of information sharing mechanisms which support the face to face sharing of meetings, using standards where available such as the Traffic Light Protocol (TLP).

Who is it shared with?

It is natural for communities to group together based on geography, culture and language and the same has happened with NSIEs who agree to share with each other. The UK-NSIE for example actively shares with the US-NSIE, which is the worlds longest running NSIE, and more recently the Canadian NSIE. There are plans to widen this out to include Australia and New Zealand. (CPNI have also stated they will help countries wanting to establish NSIEs in Europe (resources permitting)).

Continuously look for better ways to add value by exchanging information and identify other NSIEs to exchange with.

Actions to setup an NSIE

When you are convinced of the need for an NSIE, and you are aware of its vital components, you need to think about the practical strategies that you can use to get your NSIE up and running. This section looks at these strategies, which are presented as a set of action points. As before, this advice is based on the information found in our research, from countries who have successfully established an NSIE.

The groundwork

There are a number of tasks that should be carried out before creating an NSIE:

As with all initiatives, the first action is to identify a 'champion', an owner, someone or some organization who believes that an NSIE can create a win/win scenario for public and private sector organizations, enhancing resilience both for companies and the nation. This 'champion' has to be able to demonstrate the need for, and value of an NSIE.

Chief Security Officers, or their equivalents, in the network provider organization, should develop a well-justified business case for the NSIE. This should clearly explain both threats and business benefits to be gained. This might include items such as known network vulnerabilities, and their potential to lead to loss of revenue. Costs of prevention versus costs of recovery could be presented. The Regulatory and legislative positions on critical resilience might be referred to and examples could be given of NSIEs in other countries.

Government officials in the department which will interface with the NSIE should be proactive by planning for the issues which will help to promote trust. These are issues of costs, legal issues (eg freedom of information versus confidentiality), and the relationship with regulators. These can be considered and a template set up before formal approaches from network providers.

Initial Stage

Once the decision to set-up an NSIE is reasonably stable, you can begin the process of constructing the NSIE:

Identify a small number of trusted and key individuals;

Work together to agree terms of reference and mission statement for sign-off by senior management in the public and private organizations involved;

Create an outline set of rules for the NSIE. (It is possible that these rules will be revised/updated once the NSIE is running.)

[UK] *'Generic membership rules and guidelines for information exchanges are posted on a public website http://www.cpni.gov.uk/Docs/re-20040601-00395.pdf '*

Develop a distribution agreement, e.g. based on the traffic-light protocol;

Seek advice, as necessary, on the Regulatory, legislative and legal implications of the Information Exchange, noting that these will be country-specific.

Getting Started

Appointing members

It is assumed that by process of negotiation and agreement, the public and private bodies to be involved have been approached and agree to appointing members.

Many existing NSIEs have stressed that it is better to start small, and establish the principles of trust and confidentiality. When this is successful, other organisations will see the benefit of joining

The number of members per body should be kept small enough for people to get to know one another, again to engender trust. Several NSIEs researched have stressed that they do not scale easily and must be kept small. Typically, one or at most two per organization should be appointed;

Members must realise this is a personal appointment; no substitutes are allowed to attend, and they understand the obligation to give the same weight of information as they receive;

All members should sign-up to the public/private sector partnership NSIE rules and most importantly a distribution policy such as the traffic light protocol;

The chairperson/co-chairpersons should be appointed as agreed in the outline rules (or subsequent amendment).

Operational procedures

A provisional meeting schedule should be agreed. NSIEs tend to meet several times a year (eg 6 times in UK, US). This is because face to face meeting builds trust, which is crucial for the NSIE to succeed;

It is usual for the government organisation to organise each event; provide administrative support and a secretary for each event and provide a suitable venue for each event;

The meeting venue must be chosen carefully – if you choose a government building there may exemption from Freedom of Information Act (FOIA) legislation. It is also a visible indication of trust if physical security precautions are taken very seriously;

The government organisation is often responsible for collating and distributing the minutes of each event. Minutes are anonymised and given the information sharing level of AMBER. When complete, the minutes are e-mailed to the full membership of the exchange or distributed via a secure portal;

There is generally a period of **closed** exchange, restricted to NSIE membership only, for the purposes of confidential information exchange. This is followed by a period of **open** exchange for the purposes of general discussion and presentations. Visiting (i.e. non-Member) speakers may be invited by the Exchange to give specific presentations of interest to the group during the open session. (In the UK the closed session takes place in the morning and the open in the afternoon);

The agenda and time frame of the NSIE concentrates on longer term prevention of major incidents and emergencies rather than real time 'fire-fighting'.

The way forward

The need for information exchanges has often been recognised by resilience planners and information security experts. But these concerns have not always been readily accepted at senior management level without precise quantification of the impact upon their businesses.

Similarly, Government reaction is usually provoked by 'clear and present danger'. Recent terrorist activity and increases in ‘computer hacking’ have raised the resilience profile. Governments are more likely now to initiate action but members of the security community still need to be proactive in identifying and communicating specific, and quantified, critical vulnerabilities and, hopefully, roadmaps for remedial action.

Only with this preparatory groundwork will senior business champions be prepared to support the necessary activities. Our study has shown that the take-up of network security activities is greatly enhanced once very senior manager has been alerted to the dangers and to the possible remedies.

NSIEs have evolved to meet the security challenges of increasing dependency on eCommunication networks. It has not been an easy evolution with many barriers along the way but more and more countries and national organizations can see the need for sharing of information between private and public stakeholders, like the NSIE model.

Our vision is that this Guide will help to support those member states which are already aware of the mutual benefits of NSIEs and wish to establish their own Network Security Information Exchange in their countries.

We also hope that this guide will explain the benefits of NSIEs to those Member States who are in the early stages of developing their CIIP strategies and reflect on how an NSIE could be part of this strategy.

Our vision is that existing and developing national NSIEs can learn from this guide and begin to share information with each other using common approaches, policies, and methods. This could be done either at cross-country level, pan European level or even internationally.

ENISA was set up to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security problems.

In order to achieve this goal, ENISA is a Centre of Expertise in Network and Information Security and is stimulating the cooperation between the public and private sectors.

Our ultimate vision is that trusted information sharing and the NSIE model will play a vital role in preventing, addressing and responding to network and information security problems.

ENISA will promote the guide and facilitate the creation of new NSIEs at national level. The Agency will also assess the possibility of building the first trusted pan European information sharing platform on public eCommunications networks.

Appendix A- Reference

This Part of the Guide is intended to provide supporting reference information.

Organisations offering support

Several member States have expressed interest in setting up their own NSIE. The following organizations and resources may be of assistance.

ENISA has been recognised world-wide as a centre of excellence in network and information security, gives advice and recommendations to European Member States and European institutions, and acts as a switchboard of information for good practices. The agency facilitates contacts between the European institutions, the Member States and private business and industry actors. The link below gives information about ENISA's brokerage services

http://www.enisa.europa.eu/doc/pdf/FACsheets/Brokerage.pdf

Having commissioned this NSIE Guide based on observed good practice and raised awareness on the importance of information sharing through workshops, events and publications, ENISA may be able to organise brokerage events between Member States interested in establishing information sharing schemes.

Some existing NSIEs work together for mutual benefit. Representatives from the United States, United Kingdom and Canadian NSIEs have participated in trilateral meetings. The events included tri-lateral information sharing. Following the sharing session were workshops based on the security issues of NGN convergence and how all three countries can work together. Each country's NSIEs agreed to champion at least one of the issues derived from the workshops and all three countries agreed to work collaboratively with one another on these issues.

References

CPNI - Centre for the Protection of National Infrastructure, UK
http://www.cpni.gov.uk/Products/information.aspx

The website lists 10 Information Exchanges and contact details.

US-NSIE

OMNCS_- Office of the Manager, National Communication System . (2001) *Guide to Understanding The national Coordinating Center for Telecommunications and the Network Security Information Exchanges.* www.ncs.gov/nstac/reports/2000/NCC_NSIE.pdf

IAAC Information Assurance Advisory Council

Sharing is Protecting. (2003)
http://www.warp.gov.uk/Marketing/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.pdf

The IAAC report on information sharing, sponsored by NISCC (now CPNI.) This identifies many information sharing models/organisations. It was produced in 2003 but it is good background.

ENISA

Thorbrugge,M. And Gorniak, S. (2007) *EISAS- European Information Sharing and Alert System. A feasibility Study.* http://www.enisa.europa.eu/doc/pdf/studies/EISAS_finalreport.pdf

Bell Labs.

A*vailability and Robustness of Electronic Communications Infrastructures-The ARECI Study.* Brussels ; Copyright © ECSC – EC – EAEC, (2007) http://www.bell-labs.com/ARECI

This Study strongly urges European Institutions, Member States and Private Sector stakeholders to chart, and embark on, a new course of policy and practice that forcefully advocates highly available and highly robust communications infrastructure.

WARPs

Warning, Advice and Reporting Points http://www.warp.gov.uk

This site describes an information sharing model with some useful reference material for NSIEs such as the 'Why would I tell you?' report on the human aspects of building trust.
http://www.warp.gov.uk/TrustedSharing.htm#S4

European Commission DG JLS

Messaging Standard for Sharing Security Information (MS3i) http://www.ms3i.eu

This EC project objective is to develop a management messaging standard which specifies the requirements, in terms of policies, processes, and controls, for implementing, operating, maintaining

and improving the sharing of security related information. The scope is for it to be used within an organisation, between organisations, within a nation state and internationally.

Appendix B - Questionnaire

Analysis of the ENISA stocktaking document[15] identified European countries where Information Exchange activity might provide useful evidence of good practice. Questionnaires were sent and replies received from, Germany, Netherlands, Norway, Sweden, Switzerland, United Kingdom. All replies were very helpful in creating this Guide but not all currently operate a full NSIE.

The following questionnaire was used to assist compilation of this Guide on creating an Information Exchange to improve telecommunications resilience.

1. Mission statement:

Does your Information Exchange have a mission statement describing its purpose, if so would you please provide details?

2. Constitution:

How leadership is provided – who chairs/coordinates meetings?

How would you describe the structure and governance of the Information Exchange?

Briefly describe the government bodies represented in the Information Exchange, including to whom they report.

3. Membership:

Who are the typical stakeholders of your Information Exchange? How are they selected? Is there a particular profile of experts that take part in the process?

Please describe criteria for and selection of members? Do you have certain disqualification criteria if members behave abnormally?

Please describe any different levels of membership? - What is your view on optimum numbers?

What incentives do you offer to your members to share their information and knowledge?

4. Building Trust:

---

15 ENISA, (2008) Stock Taking of Member States' Policies and Regulations related to resilience of public eCommunication networks .available at: http://www.enisa.europa.eu/doc/pdf/resilience/stock_taking_final_report_2008.pdf

Please describe any codes of practice, protocols or legal frameworks which help build trust, for example Membership rules, Non disclosure Agreements or an anonymity mechanism when sharing sensitive information?

5. Interfaces:

Briefly explain the relationship and communications of your Information Exchange with other similar exchanges or bodies (e.g. emergency planning, information assurance/resilience etc)

Is the regulator part of the Information Exchange and if so what has been the impact?

Describe any links which your Information Exchange has with any other national or international Information Exchanges.

6 Funding and financing:

What are the cost implications of your Information Exchange?

Describe the extent, if any, of government funding, resource provision, web hosting etc.

7. Operational practicalities:

Describe the operational practicalities (where does it meet, who hosts meetings, how does it operate, how often does it meet?)

Who provides administrative assistance?

8. Information and Services

What kind of services does your Information Exchange offer to its members (e.g. advisory, warning, good practices development/dissemination, reporting etc)?

How are these services delivered? How do you disseminate information, vulnerabilities and preparedness measures (face-to-face meetings, email, protected website etc.)?

What information is collected and how?

If this information includes vulnerabilities, how do you validate these vulnerabilities? How do you develop new preparedness measures addressing these vulnerabilities?

9. Problems and Suggestions:

What are the major problems/barriers (if any) in running the Information Exchange? - how did you solve them?

Are there any things which you would change or which would improve in your Information Exchange?

What main piece of advice would you give to someone just starting out to create an Information Exchange?

Please tell us if you feel we have missed out any important questions or subject areas which should be addressed when producing the good practice guide.

If you have any documentation which you would be willing to share with us, or web-links to relevant information, we would be grateful to receive these as part of your answers.

Appendix C - Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) was created in order to encourage greater sharing of sensitive (but unclassified) information. The originator needs to signal how widely they want their information to be circulated beyond the immediate recipient, if at all

[UK] *'Each Representative will give each piece of information they provide, one of four 'information sharing levels', (red, amber, green, white.) All Representatives must respect the designated sharing levels of all information offered within the exchange'*
'If the Representative offering the information does not designate a sharing level, the information will be assumed to be AMBER, and the identity of the providing organization be assumed to be RED.'
'If a company is prepared to share sensitive information, but does not want to be identified, they can tell the chair in confidence. The chair will brief the meeting and anonymize the information.'

The TLP is based on the concept of the originator labelling information with one of four colours to indicate what further dissemination, if any, can be undertaken by the recipient. The recipient must consult the originator if wider dissemination is required.

The four colours and their meanings are as follows:

Personal for Named Recipients Only - In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information will be passed verbally or in person.

Limited Distribution - The recipient may share AMBER information with others within their organisation, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.

Community Wide - Information in this category can be circulated widely within a particular community. However, the information may not be published or posted on the Internet, nor released outside of the community.

Unlimited - Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.

Appendix D - Chatham House Rule

The Chatham House Rule reads as follows:

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".

The world-famous Chatham House Rule may be invoked at meetings to encourage openness and the sharing of information.

EXPLANATION of the Rule

The Chatham House Rule originated at Chatham House with the aim of providing anonymity to speakers and to encourage openness and the sharing of information. It is now used throughout the world as an aid to free discussion. Meetings do not have to take place at Chatham House, or be organized by Chatham House, to be held under the Rule.

Meetings, events and discussions held at Chatham House are normally conducted 'on the record' with the Rule occasionally invoked at the speaker's request. In cases where the Rule is not considered sufficiently strict, an event may be held 'off the record'.

http://www.chathamhouse.org.uk/about/chathamhouserule/

Appendix E - Example Non Disclosure Agreement (NDA)

GovX AMBER (when completed)

GovX NETWORK SECURITY INFORMATION EXCHANGE (NSIE)
CONFIDENTIALITY AGREEMENT (the "Agreement")

This Agreement sets forth the terms and conditions governing the exchange of Confidential Information (as defined below) among and between the members of the Govx Network Security Information Exchange (the "NSIE") and, when appropriate Guest Parties (as defined below).

Members of the NSIE, are referred to collectively as "Parties" and individually as "Party" herein.

The Parties desire to improve the security of their respective networks and systems and the overall security of the nation's critical communications infrastructure (the "Purpose"). In pursuing these aims, the Parties expect from time to time to disclose and otherwise be exposed to, certain Confidential Information.

THE PARTIES HEREBY AGREE as follows:

1 Introduction

1.1 This Agreement is to record (i) the terms upon which each Party is prepared to disclose their Confidential Information (as defined below) relating to activities undertaken in connection with the Purpose and (ii) the terms upon which each Party or Guest Party shall receive the Confidential Information . This includes, but is not limited to, information exchanged during routine NSIE meetings and specialist workshops.

2 Definitions

2.1 In this Agreement, the following words and expressions shall have the following meanings unless the context otherwise requires:

"Appointed Signatory" means the person(s) granted authority to counter-sign the Agreement on behalf of the NSIE and this will be the Government Chairperson;

"Authorised Representative" means the person granted authority to sign the Agreement on behalf of the Party or the individual that is the Guest Party;

"Confidential Information" means and includes:

a) know-how, specifications, designs, techniques, technologies, systems, codes, programs, inventions, methodologies, marketing plans relating to a Party and information of whatever nature relating to a Party and its networks, customers, businesses or financial affairs which is obtained after this Agreement is entered into and shall include information which is received either in writing or orally from or pursuant to discussions between the Parties;

b) analyses, studies, reports and other documents prepared by any Party to this Agreement which contain or otherwise reflect or are generated from any such Confidential Information as is specified in paragraph (a) above; and

c) information of a commercially sensitive nature relating to a Party obtained by observation during visits to any Party's premises;

"CPNI" means the Centre for the Protection of National Infrastructure, the Government agency sponsoring the NSIE;

"Guest Party" means a person not employed by or representing a Party, who has been invited to attend a specific NSIE meeting or workshop, and who has executed this Agreement and thus agrees to by bound thereby;

"Originator" means the Party that discloses Confidential Information under this Agreement;

"Recipient" means a Party or Guest Party that receives Confidential Information disclosed hereunder; and

"Traffic Light Protocol" (TLP) defines four agreed information sharing levels as follows:

a) RED – Disclosure of information is restricted to those present at the meeting or forum and must not be disseminated outside of the meeting or forum. In most circumstances RED information will be passed verbally or in person;

b) AMBER – Limited distribution. The Recipient Party, but not the Guest Party, may share AMBER information with others who are employed by the same Party as the Recipient Party pursuant to Section 4 below, but only on a "need-to-know" basis;

c) GREEN – Information can be shared by a Party with other organizations or bodies in the network security, information assurance or CNI community, but not published or posted on the internet; and

d) WHITE – Unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction by both Guest Parties and Parties.

2.1 The headings in this Agreement are provided for ease of reference only and shall not be taken into account in the construction or interpretation thereof.

2.2 Words importing the singular number shall include the plural and vice versa, words importing one gender shall include all genders and words importing persons shall include bodies corporate, unincorporated associations and partnerships.

3 Identification of Confidential Information

Confidential Information howsoever provided by an Originator shall be identified as such by the Originator at the time of disclosure in accordance with the TLP. All Confidential Information shall be deemed to attract a TLP level of **AMBER** unless otherwise stated or written. However, by default and unless specifically stated otherwise at the time of disclosure, the identity of the source of the Confidential Information will always be RED.

4 Confidentiality Undertaking of a Party

4.1 In consideration of the Confidential Information being made available by an Originator, each Party hereby irrevocably undertakes with the Originator and the NSIE both for itself and as trustee for, and on behalf of, its personnel which it has invited to attend a meeting or otherwise disclosed Confidential Information to, that the Party and its personnel shall:

a) only use the Confidential Information for the Purpose;

b) not store in any medium, copy, reproduce or reduce to writing any material part of the Confidential Information except as may be reasonably necessary for the Purpose; and

c) restrict disclosure of and/or access to any Confidential Information, within the framework of the TLP, to those Authorised Representatives who have reasonable need to see or use it for the Purpose and inform each of those Authorised Representatives of the confidential nature of the Confidential Information and of the obligations on the Recipient in respect of the Confidential Information and ensure its employees and other personnel comply with the confidentiality and non-disclosure obligations contained herein.

4.2 Where the Recipient is a Guest Party, in consideration of the Confidential Information being made available by an Originator, the Guest Party shall:

a) only use the Confidential Information for the Purpose; and

b) not store in any medium, copy, reproduce or reduce to writing any material part of the Confidential Information;

c) not make any disclosure whatsoever in relation to the fact that discussions or negotiations are taking or have taken place between the Parties; the content or nature of any such discussions or negotiations or any other fact in relation thereto.

4.3 The disclosure of Confidential Information by any Originator to the other Parties shall in no way be construed to imply any kind of transfer of rights connected with the Confidential Information including, without limitation, any intellectual property rights, trade marks or business secrets.

4.4 Each Recipient will treat and safeguard as private and confidential all of the Originator's Confidential Information and will take all reasonable precautions in dealing with any such Confidential Information so as to prevent any third party from having access to the Confidential Information. Recipients shall ensure that any and all copies made in furtherance of the Purpose shall bear the same notices or legends, if any, as the originals.

5 Non-disclosure to third parties

Save as otherwise expressly permitted herein, no Recipient will at any time without the relevant Originator's prior written consent:

a) disclose such other Originator's Confidential Information to any third party either directly or indirectly;

b) disclose to any person either the fact that discussions or negotiations are taking place between the Parties or the content of any such discussions or negotiations or any of the terms, conditions or other facts with respect to any other Party, including the status thereof, unless required to do so by law or by the order or ruling of a court or tribunal or regulatory body or recognised stock exchange of competent jurisdiction, in which case, if the Recipient is required to disclose such information it will, unless prohibited from doing so, notify the Originator promptly in writing of that fact and in any event, wherever legally possible prior to making such disclosure.

6 Unintended Disclosure

Each Recipient agrees that, in the event that Confidential Information is disclosed or used by them without authorisation, the Recipient shall immediately notify the Originator of the unauthorised disclosure and take all appropriate steps to prevent further dissemination of the disclosed Confidential Information and to prevent further unauthorised disclosure. The obligation to notify the Originator of any unauthorised disclosure and to mitigate damage remains in effect regardless of any other rights and obligations arising under this Agreement.

7 Limitation on further actions

7.1 It is understood that all communications regarding the Parties' discussions, requests for additional information or meetings or questions will be submitted or directed to a Party's Authorised Representatives who are subject to this Agreement.

8 Exclusion from Confidential Information

These terms and conditions will not apply to any Confidential Information which:

a) is in or becomes part of the public domain or is or otherwise becomes public knowledge by any means other than by breach by any Recipient of any obligation contained herein; or

b) was previously or is at any time hereafter disclosed to a Party by any third party having the right to disclose the same provided that such source is not known to the Recipient to be bound by a confidentiality agreement with, or other obligation of secrecy to, any other Party; or

c) is released from the provisions of this Agreement by written consent given by a director or authorised representative of the Originator.

9 Return of Confidential Information

All Confidential Information of any Originator (including all copies held by any other Party) will forthwith be returned to the Originator upon receipt by such Recipient of a written notice to that effect from the Originator, and such Recipient will (i) destroy all copies of any analyses, studies or other documents prepared by the Recipient for its use containing or reflecting, or generated from, in whole or in part, any Confidential Information relating to the Originator and (ii) expunge and destroy any such Confidential Information from any computer, word processor or other device in its possession or custody or control containing such Confidential Information and on request provide the Originator with written confirmation of the same.

10 No responsibility for information provided

Each Party and each Guest Party understands and acknowledges that no representation or warranty, express or implied, as to the accuracy or completeness of the Confidential Information is being made by the Originator(s), and that the Originator(s) will not have any liability to any person resulting from any use of the Confidential Information.

11 Publicity

Each Party and Recipient agrees that it shall not advertise or otherwise publicise the existence or terms of the Purpose, this Agreement or any other aspect of the relationship between the Parties without all Parties' prior written consent, such consent not to be unreasonably withheld.

12 Breach of Agreement

Each Party and each Guest Party acknowledges and agrees that damages may not be an adequate remedy for any breach of this Agreement and that any affected Party shall be entitled to the remedies of injunction, specific performance and other equitable relief for any threatened or actual breach of this Agreement.

13 Commencement and Termination

This Agreement shall become effective as to a Party, or Guest Party as the case may be, upon signature by the duly authorised representative of that Party or of the Guest Party and shall remain in effect with respect to that Party or Guest Party until terminated in writing by such Guest Party or Party's Authorised Representative upon notice to all other Parties and Guest Parties of not less than thirty (30) days. Upon such termination, all Confidential Information in the possession of the terminating Party (for the avoidance of doubt, no Confidential Information should be in the possession of a Guest Party) shall be returned and/or destroyed in accordance with paragraph 9 above. Notwithstanding any such termination, the rights and obligations with respect to the disclosure and use of the Confidential Information shall remain in effect for a period of five (5) years from the date of termination or for such other period agreed to, on a case-by-case basis, by each Originator and each Recipient.

14 Governing Law

These terms and conditions shall be governed by and construed in all respects in accordance with the laws of England and the Parties and Guest Parties submit to the jurisdiction of the English Courts for all purposes relating to this Agreement.

15 General

15.1 Any notice or other communication to be given under this Agreement must be in writing and may be hand delivered or sent by pre-paid first class letter post to CPNI at the address below:

The Secretary Government department

15.2 Any notice shall be deemed served if hand delivered, at the time of delivery; and if posted three (3) UK business days after posting.

15.3 CPNI will maintain a list of contact details for all Parties and Guest Parties signed up to this Agreement which each Party can access whenever required, on the Secure Extranet.

15.4 None of the Parties or Guest Parties shall assign, sub-license or otherwise transfer its rights or obligations under this Agreement without the prior written consent of each of the other Parties such consent not to be unreasonably withheld.

15.5 No failure or delay by a Party in exercising any of its rights under this Agreement shall operate as a waiver of such rights, nor shall any single or partial exercise preclude any further exercise of such rights. Any waiver must be in writing and signed by the waiving Parties to be effective.

15.6 If any provision of this Agreement is determined to be invalid in whole or part (for any reason whatsoever) the remaining provisions or parts thereof shall continue to be binding and fully operative.

15.7 This Agreement (including all appendices) constitutes the entire agreement between the Parties and Guest Parties concerning the Purpose and supersedes all previous arrangements, commitments, understandings and agreements between the Parties and Guest Parties concerning the subject matter hereof. Nothing in this paragraph 15 shall act to exclude or limit any Party's or Guest Party's liability to any other Party or Guest Party with respect to fraudulent misrepresentations. This Agreement may only be amended by an instrument in writing signed by authorised representatives of each Party.