

NISCC's Information Exchanges Example Membership Guidelines

Version 1 ~ June 2004

Contents

Section	Title.....	page
1	Terms of Reference.....	2
2	Corporate Membership Criteria.....	4
3	Personal Representative Criteria.....	5
4	Information Sharing Rules.....	6
5	Administration.....	7
6	Organisational Membership List.....	8
7	Representative List.....	9
8	Definitions.....	10
9	Acceptance Form.....	11
10	Security Check.....	12

Notice

These Guidelines are not intended as a legally-binding contract or non-disclosure agreement. Should other organisations or countries use these as a basis for the creation of an information sharing forum, they are advised to determine the legal status of such guidelines in their country as appropriate.

1 Terms of Reference

- 1.1 The UK [sector, function or technology] Information Exchange (IE) is designed to facilitate for its members the exchange of information, in a confidential and trusted environment, concerning threats, vulnerabilities and incidents of electronic attack on members' networks and environments.
- 1.2 Objectives
 - 1.2.1 To develop a trusted environment where information can be shared amongst those with responsibility for the protection of the [sector, function or technology] element of the Critical National Infrastructure (CNI).
 - 1.2.2 To provide a working forum to identify issues facilitating the unauthorised penetration or manipulation of networks or systems and supporting software that affect the CNI.
 - 1.2.3 To identify and develop mitigation for those vulnerabilities that could otherwise be exploited
 - 1.2.4 To deter attacks on the [sector, function or technology] element of the CNI through the development and implementation of best practices and Incident Response Plans
- 1.3 To engender trust and ensure that full exchange of information is achieved, each member organisation may sponsor two representatives. Only these named representatives may attend the exchange.
- 1.4 The membership shall be restricted to organisations that meet the criteria in **Section 2**.
- 1.5 Representatives from these organisations shall be required to meet the criteria in **Section 3**.
- 1.6 Both corporate members and individual representatives shall comply with the information sharing procedures and rules set out in **Section 4**.
- 1.7 The IE will be jointly chaired by a representative from NISCC and a corporate representative. IE office holders are listed at 5.7 below.
 - 1.7.1 The NISCC chair will be one of two named senior NISCC officers.
 - 1.7.2 The industry chair, and deputy chair, will be elected for a period of one year, by the IE members, as an agenda item in the Spring meeting. After a year, the Chair will relinquish the post; the Deputy will assume the Chair; and the IE members will nominate and elect a new deputy. Nominations or recommendations for these industry positions should be forwarded to NISCC in advance of the Spring meeting.

- 1.8 The IE will create, as necessary, sub-groups and working groups to take forward detailed work projects, as agreed by the IE. Membership of sub-groups and working groups will not necessarily be restricted to IE Representatives, but appointed as appropriate to the project.
- 1.9 This Exchange's "incorporation" will not be bound by a signed legal contract. However, the Exchange can review this status if a member so wishes.
- 1.10 Public information concerning the IE and its work, including membership details, is restricted to the following statement: "The IE is for [sector, function or technology]. It was formed in [date] to share confidentially mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the [...] environment. The IE includes members from UK-based [sector, function or technology] companies and NISCC." However the industry chair may, with the authority of the group, make further statements about the work achieved, when this would serve the general good.

2 Corporate Membership Criteria

- 2.1 The membership of the exchange shall be restricted to organisations that meet any of the three criteria below, and do not pose a threat to the security, confidentiality or integrity of the IE by their membership.
 - 2.1.1 Any major UK-based organisation which is [sector, function or technology] provision of critical services to the UK. Under the current UK definition of the CNI, 'critical services' are the provision of communications, energy, finance, health, government, emergency services, water, food and transport services.
 - 2.1.2 [if relevant] Any major UK-based organisation which is responsible for the safe running of a potentially hazardous industrial process. Identified hazards, under the current UK definition of the CNI, are chemical, radiological, biological, nuclear, and environmental.
 - 2.1.3 NISCC, plus any other government or police representation which the group elects.
- 2.2 Application by a company or government or police body to join the IE will be put to the existing membership for approval. Members will vote; applicants require unanimous approval to join. An existing member may only object to the applicant on grounds that they do not meet these criteria for membership.
- 2.3 The list of member Organisations is at Section 6.

3 Personal Representative Criteria

- 3.1 The membership of this Exchange shall be restricted to a maximum of two representatives from each organisation listed in Section 6. The full list of Representatives is at Section 7.
- 3.2 Only these named individuals may attend meetings of the Exchange; no substitution will be permitted.
- 3.3 The individuals' role within the organisation shall reasonably fit the remit of this Exchange as set out in Section 1.
- 3.4 Each individual Representative shall abide by the membership rules, and undertakes personally to respect the confidentiality and integrity of the IE, and information shared at its meetings. If a member breaches these rules, the IE reserves the right to terminate their membership. Termination will be effected by a motion from one member, supported by a simple majority vote.
- 3.5 With each proposal for membership, an organisation shall provide the exchange with the following personal information to provide an assurance of bona fides and engender trust relationships within the Exchange:

Full Name	Job Description
Date of Birth	Place of Birth
Nationality	Home Addresses for last 5 years
Occupation	Employer

A form is available from NISCC for this purpose.

- 3.6 Members are obliged to inform NISCC if there is a change in any information supplied under 3.5 above.
- 3.7 The procedure for gaining membership is:
 - 3.7.1 Proposal or nomination by an existing IE member by e-mail to NISCC.
 - 3.7.2 The proposed name will be circulated by NISCC to all members at least two weeks prior to the next meeting of the exchange.
 - 3.7.3 The proposal will either be confirmed or rejected by the membership at the meeting, by unanimous vote. An existing member may only object to the applicant on grounds that they do not meet these criteria for membership.
 - 3.7.4 Subject to passing a security check, a successful new Representative will attend the following meeting.
- 3.8 Non-attendance. A member organisation may be asked to leave the exchange if neither of its representatives attends three successive meetings.

4 Information Sharing Rules

- 4.1 Sensitive information will be shared orally in the ‘closed’ part of the Exchange’s meeting. Each Representative will give each piece of information they provide one of four ‘information sharing levels’, in accordance with their wishes for the handling of their information by other Representatives. The four Information Sharing Levels are:
- 4.1.1 **RED** Non-disclosable Information and restricted to representatives present at the meeting themselves only. Representatives must not disseminate the information outside of the exchange. RED information may be discussed during a meeting, where all representatives present have signed up to these rules. Guests & others such as visiting speakers who are not full members of the Exchange will be required to leave before such information is discussed.
 - 4.1.2 **AMBER** Limited Disclosure and restricted to members of the IE; those within their organizations (whether direct employees, consultants, contractors or outsource-staff working in the organisation) who have a need to know in order to take action.
 - 4.1.3 **GREEN** Information can be shared with other organizations, Information Exchanges or individuals in the network security, information assurance or CNI community at large, but not published or posted on the web.
 - 4.1.4 **PUBLIC** Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member may publish the information, subject to copyright.
- 4.2 It is the responsibility of all Representatives to respect the designated sharing levels of all information offered within the exchange.
- 4.3 It is the responsibility of the Representative offering the information to specify its sharing level. If the Representative offering the information does not designate a sharing level, the information will be assumed to be AMBER, and the source [identity of the providing organization] be assumed to be RED. If any Representative has any doubt whether information is RED, he/she must contact the person who offered it before taking any action on it.
- 4.4 If preferred, RED or AMBER information may be briefed in to the exchange anonymously via NISCC, or either joint-chair.
- 4.5 This exchange is not a mechanism for passing information about possible criminal activity to the police.
- 4.6 Within the Exchange, Representatives may not identify current or former employees suspected or accused of hacking, unless they have been convicted and it is public knowledge.

5 Administration

- 5.1 Unless alternative arrangements have been agreed by the IE, NISCC will:
- 5.1.1 organise each event;
 - 5.1.2 provide administrative support and a Secretary for each event; and
 - 5.1.3 provide a suitable venue for each event.
- 5.2 Minutes of Meetings. The NISCC will be responsible for collating and distributing the minutes of each event. The minutes of the meeting will record attendance and apologies received. The minutes of each event will be anonymised and given the information sharing level of AMBER as set out in Section 4 above. When complete, the minutes of each event will be e-mailed to the full membership of the exchange.
- 5.3 Meetings of the exchange will typically take the following structure:
- 5.3.1 A period of **closed** exchange, restricted to the nominated membership only, for the purposes of confidential information exchange. Attendance will be expected of at least one representative of each organisation.
 - 5.3.2 A period of **open** exchange for the purposes of general discussion and presentations. Attendance will be at the discretion of each representative. Visiting (i.e. non-Member) speakers may be invited by the Exchange on occasion.
- 5.4 Each representative shall ensure that they have an appropriate means of identification when attending an event. Appropriate means of identification may include driving licence, company pass, Bankers Card etc.
- 5.5 Each representative shall ensure that they deposit with the event administrator all items having recording or transmitting capability, such as cameras, mobile telephones, electronic organisers, PDA's, walkmans, laptop computers etc.
- 5.6 If for any reason a representative is unable to attend an event, they should notify the Exchange Administrator as soon as possible.
- 5.7 Contact information for IE office holders.

Name	Role for IE	Telephone	Email
	Government Co-Chair		
	Government Co-Chair		
	Industry Chair		
	Industry Deputy-Chair		
	IE Secretary		
	IE Secretary		
	Administration contact point		
UNIRAS	24X7 Response		uniras@nisc.gov.uk
NISCC Conference call number			

6 Organisational Membership List

6.1 List of Companies

Company Name

Company Name

Company Name

6.2 Government

NISCC

7 Representative List

Sector	Company or Organisation	Name
	List of members	

8 Definitions

Member Organisation	any corporate body (public or private), partnership or unincorporated association that meets the criteria for membership of the IE as set out in section 3.
Representatives	any person representing their employing organisation that meets the criteria for membership of the IE as set out in section 4.
NISCC	The UK Government's National Infrastructure Security Co-ordination Centre. See www.niscc.gov.uk .
CNI	Critical National Infrastructure. The CNI is defined as those parts of the United Kingdom's infrastructure for which continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening serious economic or other grave social consequences for the community, or any substantial portion of the community, or would otherwise be of immediate concern to the Government. See www.niscc.gov.uk
BS7858	British Standard 7858 Code of practice for security screening of personnel employed in a security environment. See www.bsi.org.uk
Non-Disclosable Information	Information that must not be shared by members, but with the explicit approval of the source/provider may be used to inform a member's actions to protect their organisation.
Limited Disclosure Info	Information that may be acted upon by members but is restricted to the member organisations employees, consultants or contractors with a need to know.

9 Acceptance Form

- 9.1 I, the undersigned, have read and understood the attached Membership Guidelines of the Information Exchange. I agree these as guidelines to my engagement with this group.
- 9.2 I also understand that should I, or my parent company/organisation, fail to abide by the Membership Guidelines either I and or my parent company/organisation may be asked to leave the IE.

Name: _____

Company: _____

Signature: _____

10 Security Check

- 10.1 Some of the information shared inside IE will have a degree of sensitivity attached to it. In order to protect national security interests NISCC will carry out limited checks that do not equate to any form of official government vetting.
- 10.2 Corporate Security Screening.
- 10.2.1 Eligibility criteria for corporate membership are as stated in section 2.
 - 10.2.2 NISCC will perform a security check on the company/organisation. No information about the NISCC check will be disclosed.
 - 10.2.3 Representatives Security Screening.
 - 10.2.4 Procedures for representative membership of the IE are as stated in section 3. The details of the check is as follows:
 - 10.2.5 Each company/organisation must ensure that checks for their representatives detailed in Annex B have been successfully completed in accordance with BS 7858. The representative's company/organisation shall be responsible for managing this process.
 - 10.2.6 Once completed the Security Manager or an appropriate officer from each company/organisation shall inform NISCC that their representatives have successfully completed a BS 7858 check and will supply NISCC with the information listed at 3.5 above.
 - 10.2.7 On receipt of this information NISCC will arrange for the representative to be checked against the appropriate databases. No information about the NISCC check will be disclosed.
 - 10.2.8 On successful completion of this check representatives will be formally invited to join the IE and to sign the Acceptance Form (Section 9).
 - 10.2.9 In the event of a representative failing the BS 7858 check or the NISCC check, the representative cannot take any part in the IE.
- 10.3 Each check will be subject to review every two years.