CPNI
Centre for the Protection of National Infrastructure

CPNI INFORMATION EXCHANGE

MEMBERSHIP GUIDELINES

APRIL 2010

Terms of reference

Purpose

The UK Information Exchange is designed to facilitate the exchange of information between its members, in a confidential and trusted environment, concerning threats, vulnerabilities and incidents of electronic attack on members' networks and environments.

Objectives

To develop a trusted environment where information can be shared amongst those with responsibility for the protection of the sector element of the Critical National Infrastructure (CNI).

To provide a working forum to identify vulnerabilities that could facilitate the unauthorised penetration or manipulation of networks, systems and supporting software that affect the CNI.

To identify and develop mitigation for those vulnerabilities that could otherwise be exploited.

To deter attacks on the sector element of the CNI through the development and implementation of best practice and Incident Response Plans.

Membership

To engender trust and to ensure that full information exchange is achieved, each member organisation may sponsor up to two representatives. Only those named representatives may attend the Exchange.

Corporate membership shall be restricted to organisations that meet the criteria in **Section 2**. Representatives from these organisations shall be required to meet the criteria in **Section 3**. Both corporate members and individual representatives shall comply with the information sharing procedures and rules set out in **Section 4**.

Chair

The information exchange will be jointly chaired by a representative from CPNI (the Centre for the Protection of National Infrastructure) and a corporate representative. IE office holders are listed below.

The CPNI chair will be one of two named senior CPNI officers.

The corporate chair, and a corporate deputy chair, will be elected for a period of one year, by the IE members. 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 CPNI in advance of the meeting involving the elections.

Working groups

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.

Contract

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.

Publicity

All information concerning the IE and its work, including membership details, will not be made public, with the exception of the following statement: "The IE is a forum specifically for the sector. It was formed in 00/00 to share, in confidence, mutually beneficial information regarding electronic security threats, vulnerabilities, incidents and solutions in the UK sector environment. The IE includes members from sector companies and CPNI."

Corporate membership criteria

Corporate membership

The membership of the exchange shall be restricted to organisations that meet the criterion below, and do not pose a threat to the security, confidentiality or integrity of the IE by their membership.

Corporate criterion

Any major organisation which operates within the UK sector and contributes to the UK CNI.

Government membership

Government representation on the IE is by CPNI, the Centre for the Protection of National Infrastructure.

Approval of membership application

Application by a company or organisation 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 on grounds that the applicant does not meet the corporate criteria for membership.

Membership list

The list of member organisations is at Section 6.

Personal representative criteria

Number of representatives

The membership of this Exchange shall be restricted to a maximum of three representatives from each organisation listed in Section 6. The full list of Representatives is at Section 7.

Criteria

Only these named individuals may attend meetings of the Exchange; no substitution will be permitted.

The individuals' role within the organisation shall reasonably fit the remit of this Exchange as set out in Section 1.

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 representative breaches these rules, the IE reserves the right to terminate their membership. Termination will be by a motion from one representative, supported by a simple majority vote.

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 (a form is available from CPNI for this purpose):

Representatives are obliged to inform CPNI if there is a change in any information supplied above.

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

Representative membership application

New members will be proposed or nominated by an existing IE member, by e-mail to CPNI.

The proposed name will be circulated by CPNI to all members at least two weeks prior to the next meeting of the Exchange.

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 the above criteria for membership.

Subject to passing a security check, a successful new representative will attend the following meeting.

Information sharing rules

Sharing information

Sensitive information will be shared orally in the ‘closed’ part of the Exchange’s meeting (see section 5 below).

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.

Information sharing levels

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.

AMBER - Limited disclosure and restricted to members of the Information Exchange; 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.

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.

WHITE - Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member may publish the information, subject to copyright.

Responsibilities

It is the responsibility of all representatives to respect the designated sharing levels of all information offered within the Exchange.

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 identity of the source will be assumed to be RED. If any representative has any doubt whether information is RED, he/she must contact the person who offered the information before taking any action on it.

If preferred, RED or AMBER information may be briefed in to the Exchange anonymously via CPNI, or either joint-chair.

This Exchange is not a mechanism for passing information about possible criminal activity to the police.

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.

Administration

CPNI role

Unless alternative arrangements have been agreed by the IE, CPNI will:

- organise each event;
- provide administrative support and a Secretary for each event;
- provide a suitable venue for each event.

Minutes of meetings

CPNI will be responsible for collating and distributing the minutes of each event. The minutes 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.

Sharing of information with other exchanges

Information on incidents (in anonymised form) will be shared with other Exchanges or groups if approved by the membership of the Exchange.

Meeting structure

Meetings of the exchange will typically take the following structure:

- 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.

- 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.

Identification

Each representative shall ensure that they have an appropriate means of identification when attending an event. Appropriate means of identification must be a recognised photo id.

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, PDAs, personal stereos, laptop computers etc.

Attendance

If for any reason a representative is unable to attend an event, they should notify the Exchange Administration contact point as soon as possible.

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 2.

Representative

Any person representing their employing organisation that meets the criteria for membership of the IE as set out in sections 2 and 3.

CPNI

The Centre for the Protection of National Infrastructure. See www.cpni.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.cpni.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.

Acceptance form

I, the undersigned, have read and understood the attached Membership Guidelines of the Information Exchange (IE). I agree to abide by the guidelines in my engagement with this group.

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/Organisation:
Primary/Alternative representative *(Delete as appropriate)*
Signature:

Date: **Membership guidelines version:**

Once completed, the applicant should mail this form to the following address:

Central Support
PO BOX 60628
London
SW1P 9HA

Security check

Background

Some of the information shared inside IE will have a degree of sensitivity attached to it. In order to protect national security interests, CPNI will carry out limited checks that do not equate to any form of official government vetting.

Corporate security screening

Eligibility criteria for corporate membership are as stated in section 2.

CPNI will perform a security check on the company/organisation. No information about the CPNI check will be disclosed.

Representatives' security screening

Procedures for representative membership of the IE are as stated in section 3.

The detail of the security check is as follows:

- Each company/organisation must ensure that a check for each of their representatives detailed in Annex B has been completed successfully in accordance with BS7858 or a similar or suitable standard. The representative's company/organisation shall be responsible for managing this process.
- Once this check has been completed the Security Manager, HR or Personnel Manager (or other appropriate officer) from the company/organisation shall return both parts of the completed Security Questionnaire to each representative. The representative shall send the completed forms to CPNI.
- On receipt of this information, CPNI will arrange for the representative to be checked against the appropriate databases. No information about the CPNI check will be disclosed.
- On successful completion of this check, representatives will be formally invited to join the IE and to sign the Acceptance Form (Section 9).
- In the event of a representative failing the BS7858 (or similar) check or the CPNI check, the representative cannot take any part in the IE.

Review

Each security check will be subject to review every two years.