APCERT POC Arrangements Policy

Background

1. The APCERT POC Arrangements have been established to provide a framework for sharing information about serious and time critical computer threats and vulnerabilities by APCERT members within the APCERT region.

Purpose

2. The APCERT Point of Contact (POC) Arrangements are designed to provide a POC for APCERT members who wish to communicate with each other about:

a) serious and time critical computer security incidents and/or computer security issues for the purposes of helping to resolve or investigate an incident; and/or

b) serious and time-critical computer security vulnerabilities, knowledge of which is not yet in the public domain; and/or

c) serious and time-critical computer security threats in order to provide early warning to the POC's constituents and/or to other POCs within its regional CERT/CSIRT group. An example of this is a newly discovered fast spreading Internet worm.

3. Each economy that is a member of APCERT will propose one CERT/CSIRT that is a member of APCERT to be the POC for that economy. Full members are preferred, however, in the absence of an eligible full member within an economy a general member may be a POC (see the Guidelines). The nominated team will provide POC details to APCERT and the APCERT SC will accept and endorse the nomination.

APCERT POCs undertake to work with:

a) other APCERT POCs; or

b) other APCERT Full Members; or

c) other APCERT General Members.

4. The purpose of the POC arrangement is to provide a single point of contact between economies in the Asia-Pacific region. The APCERT POCs are required to:

a) be available and contactable on a 24x7 basis

b) provide generic telephone contact numbers, e-mail addresses and PGP keys for the POC and SMS-compatible telephone numbers where possible.

c) have backup arrangements in place to support the POC arrangements

d) POCs need to provide English-speaking contacts where possible

e) have escalation procedures in place so that immediate action can be undertaken or be able to gain appropriate authorisation for action with minimal delay.

5. APCERT will provide a single e-mail distribution list of all POCs.

6. All contact details for the POC arrangements for APCERT will be posted on the APCERT secure web site. It is the responsibility of all participating APCERT teams to ensure that the POC details are up to date at all times. This can be done by forwarding an email to apcert-poc@auscert.org.au.

APCERT POC Arrangements Policy

Restrictions on use of the POC Arrangements

7. Use of the POC Arrangements will be restricted to APCERT members in Asia-Pacific economies. Do not publish POC arrangements and contact details on any publicly accessible web site or otherwise make them available to other parties outside of APCERT.

Action to be taken by the POC

8. In responding to requests for assistance, through the POC Arrangements (for the purposes outlined in paragraph 2(a) above):

a) The POC undertakes to assist the originating reporting party to resolve an incident as far as possible within the POC's own policy guidelines, powers, capabilities (including resource constraints) and legal constraints and taking into consideration its other priorities.

b) The POC undertakes to contact other parties within its constituency in order to provide the assistance required or to inform relevant parties where appropriate about the alleged incident.

c) If it is not possible to provide some or all of the assistance requested of the POC for any reasons, then the POC should inform the originating requesting party of the extent of its ability to assist, if at all.

d) It is the responsibility of the POC to establish and maintain effective contact arrangements with other CSIRT/CERT teams that are either Full or General Members of APCERT within in their economy.

e) The POC is responsible for establishing and maintaining any other necessary contact arrangements with other organisations in their economy (for example, law enforcement agencies if appropriate).

9. When an APCERT POC receives information about a serious and time critical computer security threat or vulnerability (as described in paragraphs 2(b) or (c) above) and the POC is able to, or is permitted to, share this information with other APCERT members, then the APCERT member POC should do so by contacting each APCERT POC within APCERT.

10. Where the original reporting party allows the POC to use its discretion as to which organisations and/or POCs the information can be passed, then the POC should only pass sensitive information (of the type outlined in paragraph 2(b) above) to those that it trusts to abide by the information handling caveats.

Prioritisation

11. When an APCERT CSIRT receives requests for assistance, either through the POC Arrangements, (for the purposes outlined in paragraph 2(a) above), or from any other party, either part of APCERT or not, priority should be given to requests for assistance from:

1st APCERT POCs

2nd APCERT members

3rd External CSIRTs accepted as part of the APCERT POC Arrangements

APCERT POC Arrangements Policy

Timeliness

12. In seeking to share information about a serious and time-critical computer security threat or vulnerability, the POC should endeavour to do so as soon as possible/practical, taking into consideration the urgency of the information and the likelihood that the threat/vulnerability could have an immediate or imminent and widespread impact on networks within the regional CERT/CSIRT group to which the POCs belong.

Honour Information Handling Caveats Imposed by the Originating Reporting Party

13. The CERT/CSIRT acting as a POC agrees to abide by any information handling caveats imposed by the originating reporting party.

14. Where a POC is permitted to communicate with third parties about the information provided by the originating reporting party, the POC will ensure that the recipients are aware of the information handling caveats that apply to the information, and where possible, seek their agreement to abide by them. See also paragraph 9 above.

15. In the case of information being provided to a POC for the purposes outlined in paragraph 2(b) above, the POC should not pass information to any other third parties, even if it is permitted to do so, unless the POC has a trusted relationship with the third party and only if the trusted third party agrees to abide by the information handling caveats before the information is passed.

16. Generally, originating reporting parties should not impose restrictions on POCs as to whom or which organisations they can pass information within their economy about serious and time-critical threats (as outlined in paragraph 2(c) above).

Breaches of Handling Caveats

17. Honouring information handling caveats is vital if CERT trust relationships are to work. This is particularly important when sharing information about computer vulnerabilities which are not yet public knowledge.

18. Generally, if POCs are abiding by the terms of paragraph 14 above breaches of information handling caveats should be rare or non-existent. However, even with the best efforts by POCs, sometimes breaches may still occur.

19. Where information is disclosed which suggests a breach of the handling caveats imposed by the originating party may have occurred, this should be brought to the attention of the POCs which had access to that information. Enquiries should be made by the relevant POCs to determine if a breach occurred within their economy, and if so, how it may have occurred. If a breach is confirmed, then the relevant POC should seek and provide an explanation to the affected parties and to the APCERT Steering Committee.