

## TF-CSIRT Terms of Reference

(Approved by the TTC on 15 July 2008)

1. A Task Force is established under the auspices of the TERENA Technical Programme (<http://www.terena.nl/about/tech/ToR.html>) to promote collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. It will be known as TF-CSIRT (Collaboration of Security Incident Response Teams).
2. The aims of the Task Force will be:
  - 2.1 to provide a forum for exchanging experiences and knowledge;
  - 2.2 to establish pilot services for the European CSIRTs community;
  - 2.3 to promote common standards and procedures for responding to security incidents;
  - 2.4 to assist the establishment of new CSIRTs and the training of CSIRTs' staff;
  - 2.5 to co-ordinate other joint initiatives;
  - 2.6 to provide a vehicle for CSIRTs in Europe to liaise with the European Commission and other policy making bodies.
3. The Task Force will focus its activities on Europe and neighbouring countries and on (potential) CSIRTs operated by national and international research and education networks, commercial Internet Service Providers (ISPs), companies, governmental institutions, as well as vendor-product teams and commercial CSIRTs. It will collaborate with other teams and organisations outside its geographical area whenever such collaboration will assist in achieving the aims of the Task Force.
4. With a commitment to the development of collaboration between CSIRTs as defined above, participation in the Task Force will be open to individuals, subject to the agreement of the Task Force chairman.
5. The chair of the Task Force will be Lionel Ferette. He will be responsible for preparing the agenda for each meeting and for co-ordinating the work of the Task Force. He will also be responsible for ensuring that any agreed deliverables are produced. The deputy chair of the Task Force will be Kauto Huopio, who will be responsible for chairing a meeting if the chair cannot participate.
6. The secretary of the Task Force will be appointed by TERENA. He/she will be responsible for taking the minutes at each meeting and for making logistical arrangements as necessary.
7. The Task Force will operate with a (renewed) two-year mandate, starting 15 May 2008. This mandate may subsequently be renewed by the TERENA Technical Committee (TTC), but if not renewed, the Task Force will be dissolved. The Task Force may also be dissolved if the TTC considers that it is making insufficient progress, its activities are no longer useful or relevant, or if the Task Force chair resigns and no replacement can be found.
8. The Task Force will meet at approximately four-monthly intervals. Physical meetings will be held at various locations, taking care to reduce overall costs to participants.
9. Reports and results of Task Force activities will be placed in the public domain, with the exception of information that is subject to copyright restrictions, has been provided on a non-disclosure basis, or where public disclosure would jeopardise the security of organisations or networks involved.
10. The Task Force will have a mailing list ([tf-csirt@terena.org](mailto:tf-csirt@terena.org)) and a web page (<http://www.terena.org/activities/tf-csirt/>) to facilitate communication amongst Task Force participants.

## Work Items

*Please note that former Work Item I has been dropped, whilst Work Items N and O are new additions.*

- A. Meetings and seminars  
A half- or one-day seminar shall normally be held in conjunction with Task Force meetings, in which experiences may be exchanged and issues of common interests for CSIRTs discussed.
- B. Trusted Introducer  
The Task Force will liaise with the Trusted Introducer (TI) service, which is subcontracted by TERENA to a professional organisation. The TI provides a form of accreditation to CSIRTs and provides various services to them. The TI will also organise regular meetings of representatives of accredited CSIRTs in conjunction with TF-CSIRT meetings. Major developments in the TI services will be reported to the Task Force.
- C. Security Contact Information for Internet Resources  
The Task Force will support the deployment of abuse contact lookup mechanisms in Regional Internet Registries. It will also help to improve documentation, propose changes in technology and procedures as appropriate, and review any privacy and data protection regulations that relate to this.
- D. Clearinghouse for Incident Handling Tools  
The Task Force will maintain a web-based clearinghouse for security software, covering both free software and commercial products. The focus of the clearinghouse will be on tools that are in actual use in CSIRTs, whose staff members participate in TF-CSIRT. Developments in the clearinghouse service will be reported to the Task Force.
- E. Training of (staff of) CSIRTs  
The Task Force will review the needs for specific training for staff members of CSIRTs and will promote the development and delivery of appropriate training materials to meet these needs. The Task Force will receive reports on the TRANSITS trainings organised by TERENA and other organisations, and on the measures that are taken to guarantee the continuity of the TRANSITS training effort.
- F. Assistance to the establishment of new CSIRTs  
The Task Force will develop and maintain appropriate resources and services to assist the establishment and development of new CSIRTs. Where appropriate, this will be undertaken in collaboration with other groups or organisations working in this area.
- G. Collaboration with FIRST and organisations in other world regions  
The Task Force will investigate possibilities to collaborate more actively with FIRST, and with counterparts of TF-CSIRT in other continents (e.g. APCERT and OIC-CERT).
- H. Request Tracker for Incident Response  
The Task Force will provide a forum (the RTIR Working Group) for collaboration on modifications and new features to the RTIR (Request Tracker for Incident Response) tool, and as a repository for knowledge about the tool and its use. This working group will also produce documentation and training material.
- J. Collaboration with the Joint Research Activity "Security" in the GN2 project.  
The Task Force will collaborate with the Joint Research Activity "Security" (JRA2) in the GN2 project, and any successor activity in any follow-up project. JRA2 will hold its meetings in conjunction with TF-CSIRT meetings wherever possible, and joint meetings between TF-CSIRT and the JRA2 team may also be organised. The chairman of TF-CSIRT and the leader of the JRA2 activity will also appoint the members of a JRA2 advisory panel. Progress reports from JRA2 will be presented to the Task Force.
- K. Liaison with the European Commission  
The Task Force will exchange information with relevant European Union bodies and advise them as appropriate. This will include the European Commission services responsible for EU policies

and actions related to data and network security, and ENISA. Meetings between TF-CSIRT deputations and relevant Commission officials will be organised as necessary.

- L. Liaison with the E-CoAT  
The Task Force will investigate whether some or all of the E-CoAT (European Co-operation of Abuse fighting Teams) activities might be integrated in the TF-CSIRT Work Programme.
- M. Incident handling and security guidelines for Grids  
The Task Force will identify, monitor and liaise with security developments in Grid communities to encourage the adoption of good security and incident management practice. Results will be reported to the Task Force.
- N. Drill Exercises  
The Task Force will investigate and possibly coordinate practical security exercises between CSIRTs. The aim is to investigate any problems and weaknesses, whilst helping improve incident handling techniques.
- O. Evaluation of new tools  
The Task Force will evaluate and review software tools that can be utilised for incident handling purposes. These will be presented and discussed at TF-CSIRT meetings.