Minutes of the 8th TF-CSIRT meeting
Zagreb, 24 January 2003

[Please note that a seminar was held the previous day. All presentations can be found at http://www.terena.nl/tech/task-forces/tf-csirt/meeting8/tf-csirt8th_progpres.html]

1. Approval of Minutes

The minutes of the last meeting held on 27 September 2002 were approved.

2. Actions from last meeting

05-07 Ian Bryant to check NATO's interest in conducting special training and assisting establishment of new CSIRTs in the EU and countries of the Former Soviet Union.
Ongoing.

06-01 Gorazd Bozic to finish forming teams for each deliverable in the new TF-CSIRT Terms of Reference.
On agenda: see agenda item 9.

06-02 Jan Meijer to initiate discussion on deliverable H (Common Incident Handling Procedures and requirements for Incident Handling Systems).
On agenda: see agenda item 9.

07-01 Gilles André to send his short document on infrastructure backup to TF-CSIRT list.
Done.

07-02 Gilles André to give presentation on infrastructure backup in next TF-CSIRT meeting.
The presentation was given in the seminar on 23 January 2003. See agenda item 8.

07-03 Wilfried Wöber/Ulrich Kiermayr to write document on how to use the IRT object in the RIPE database.
Wilfried Wöber gave a presentation in the seminar on 23 January 2003. He will expand on this presentation and collaborate with the TI team to produce the documentation (rather than a document).

07-04 Gorazd Bozic to initiate discussion on the TF-CSIRT mailing list on what to store on the password-protected part of the TF-CSIRT website.
Done.

07-05 Kevin Meynell to create password-protected part of website with initially one password for all.
It was determined that there was currently no requirement for this.

07-06 David Parker to send to TF-CSIRT mailing list the document (discussed between accredited teams) on which information can be shared between CSIRTs (in the context of Deliverable I).
Done.

07-07 All to send to Kevin Meynell URLs of projects that are relevant to CSIRTs, to be listed on the TF-CSIRT webpages
Kevin Meynell had not received any URLs to date; he will send a reminder to the mailing list.

07-08 Michel Miqueu to discuss arrangements for EISPP workshop adjacent to TF-CSIRT meeting in Warsaw in May 2003.
Done; see agenda item 4.3.

07-09 Jacques Schuurman to find out how Regionalisation Task Force kick-off document can be made available to TF-CSIRT members.

Done.

07-10 David Crochemore to ask FIRST Steering Committee if Regionalisation Task Force kick-off document may be distributed widely.

Done.

07-11 Don Stikvoort and BCP WG to finalise Don Stikvoort's document on BCP in CSIRTs.

Ongoing. Is planned for 1 March 2003.

07-12 BCP WG to prepare presentation for managers.

Ongoing.

3. Trusted Introducer Service

3.1. Status Report

Don Stikvoort reported on the activities of the TI team. A number of services were being provided for accredited CSIRTs, including a restricted website, four-monthly active maintenance, an up-to-date PGP key ring and formal signing of keys, contact information in CSV format, trusted mailing lists for information exchange and discussion, and automatic registration and maintenance of IRT objects in the RIPE database.

Two new CSIRTs had been accredited: S-CERT (Deutsche Sparkasse bank) and KCSIRT (Kennisnet, Dutch schools).

The last meeting of the accredited teams had been in September 2002 in Syros, Greece where a new review board had been elected. Since then, retroactive registration of IRT objects had been undertaken (October 2002), revision of the terminology started (November 2002), the invitation package rewritten (December 2002), and a formal key signing session held (January 2003). They had also agreed to document the IRT object in collaboration with Wilfried Wöber (February 2003). The TI website (http://ti.terena.nl) was being re-designed, and the new site would become "live" within a few weeks.

3.2. Report from TI Review Board

Karel Vietsch reported on the meeting of the TI Review Board that was held the previous day.

Andrew Cormack had been elected chairman until September 2003. His terms of office as a member of the board would expire then, and the meeting of accredited teams that would take place at that time would elect a new member to fill the vacancy on the board. The board would then meet immediately after that meeting to appoint a new chairman from amongst their numbers, and that person would hold office until September 2004. The current board would produce procedures for the election of new board members, which would be circulated well before September 2003.

The board discussed the action that should be taken by TI if it receives information that a CSIRT is no longer in business. It was resolved that in such cases TI will bring forward the periodic check for information and escalate the matter in the event of no satisfactory reply sooner then they would otherwise. The board would be informed of the action taken, as well as the outcome. It was also resolved that TERENA should undertake action against any accredited CSIRT not paying an invoice for the TI service within four months from receiving it, and if necessary propose to the board to revoke that team's accredited status.

In addition, the board discussed other TI activities including the new website that was due to be up in the next few weeks, PGP key signing that was undertaken the previous day, use of the IRT object in the RIPE database, and various mailing lists for accredited teams.

It was generally felt that meetings of accredited teams should be better prepared with minutes circulated shortly afterwards. One meeting per year was not felt to be enough, but additional meetings should only be held if there were enough relevant issues to warrant them. It was suggested that a

meeting of the accredited CSIRTs could be held in May in Warsaw, provided there were enough interesting agenda items by early April.

The next meeting of the board will be held on 29 May 2003, adjacent to the TF-CSIRT meeting in Warsaw. This would also undertake the annual review.

Gorazd Bozic asked whether the accredited team record was publicly available, and what would happen if the status of a team was downgraded. Don Stikvoort replied this had not yet been decided, but it would be a decision for the board.

Andy Bone said this should be discussed at the next meeting of the accredited CSIRTs. There needs to be a defined process for joining and removing, even though this should not be too bureaucratic.

4. Update on EC funded projects

4.1. TRANSITS

Karel Vietsch gave an overview of the TRANSITS project. This project, which has TERENA and UKERNA as its formal partners, runs from July 2002 until June 2005.

The project is contracted to produce training course materials (initially by mid-2002, with a revision by early-2004) and to run six training workshops (in spring and autumn each year). There is also some budget to partly cover the expenses of participants from the 'poorer' European countries. Karel Vietsch (TERENA) is the project manager, Andrew Cormack (UKERNA) is responsible for the course materials and the workshop programmes, whilst Raquel Corredoira (TERENA) is handling the workshop logistics.

The training course material was completed in September 2002. This remains the copyright of TERENA, but it may be used for non-commercial training courses, provided permission is sought and both TF-CSIRT and the European Commission's IST programme are credited.

A trial training workshop had already been held before the start of the project in January 2002 in Farsta, Sweden, but the first training workshop proper was held on 31 October and 1 November 2002 in Oegstgeest, the Netherlands. This attracted 21 participants from 14 countries, of whom 15 were from existing CSIRTs, and 6 were from organisations planning to establish a CSIRT. The workshop received some very positive feedback.

The next training workshop would be held on 27-28 May 2003 in Warsaw, Poland (hosted by CERT Polska / NASK), in conjunction with the 9th TF-CSIRT meeting. This would be announced on 20 February, and requests for participation must be received by 11 April. The successful applicants would be notified by 23 April, and the deadline for payments would be 14 May. It was also hoped that some of the workshop participants would stay on for the TF-CSIRT meeting.

Jacques Schuurman suggested that the TRANSITS website should be linked from the TERENA website. Karel Vietsch agreed that TERENA should link to all the IST projects they were involved with from their website.

ACTION 08-01. Karel Vietsch to ensure the TRANSITS website is linked from the TERENA website.

4.2. eCSIRT.net

Don Stikvoort reported on the eCSIRT.net project, which aims to develop a standardised way exchanging incident-related information.

Work Package 2 was currently developing a format for data storage and exchange based on IODEF/IDMEF, a common language for describing incidents, and a code of conduct. Work Package 3 would trial these developments, Work Package 4 would establish a clearinghouse for integrating and presenting incident statistics, whilst Work Package 5 would develop techniques for providing early warnings based on this integrated incident reporting.

Gilles André asked whether the project results were subject to intellectual property restrictions. Don Stikvoort replied that all results would be publicly available.

4.3. EISPP

Michel Miqueu reported on the EISPP project. This started in June 2002 with the aim of establishing a European CSIRT network of expertise, and to set up a framework to provide SMEs with adequate security services (as outlined in the 6th TF-CSIRT meeting).

WP3 involved four CSIRTs and had agreed a common advisory format based on XML (see http://www.eispp.org/documents/). Advisory exchanges using a native format had commenced in October 2002 but exchanges using this common format were expected to start in March 2003. Vulnerability assessment sharing would also start at the same time.

A workshop was planned for 28 May 2003 in Warsaw, Poland in conjunction with the 9th TF-CSIRT meeting. This was open to all European CSIRTs and would be used to discuss the current achievements of the project.

Andrew Cormack asked whether the project had spoken with RUS-CERT in Stuttgart about CAIF (the Common Advisory Interchange Format). Michel Miqueu replied they had.

5. Update on FIRST

Jacques Schuurman reported that FIRST had passed a motion at their 2002 AGM to establish a task force on regionalisation. This was an open group that aimed to find out what regional coordination efforts there were, and how FIRST can assist those.

The discussion was based on a kick-off document that outlined six main threads: real-time operational issues, information sharing, cyberdefence, policymaking and strategic planning, facilitating bilateral contacts, and trust management. A meeting had been held on 8 October 2002 in Chicago, and a further meeting would be held on 11 February 2003 in Uppsala. There would be additional meetings and teleconferences as required, with conclusions formulated by the end of March 2003. Further actions may be undertaken at the 2003 AGM in Ottawa.

The meeting in October was attended by ten people, from Europe (4), Latin America (1), North America (3) and the Asia-Pacific (2) region. There were many different views on how to proceed with each of the threads, as well as more general issues such as the overall role played by FIRST.

In the area of operations, neighbouring teams had already developed cooperation and it was unclear how FIRST might improve on this. With respect to information sharing, the need for various levels of trust and clear guidelines may mean that FIRST has some role to play there. Cyberdefence usually required links with government institutions and it was felt FIRST should generally keep out of the political arena, although they might provide guidelines and advice. Policymaking was usually connected to operational issues, whilst bilateral contact was an issue for the parties concerned. Finally, trust management may be an area where FIRST can play an important role as trust broker. However, a multi-layered membership scheme similar to the TI model would need to be introduced.

Unfortunately, after the initial exchange of ideas, there was little further progress on these issues. The task force was due to report back to the FIRST Steering Committee in March 2003, but the meeting in February did not yet have a chairman.

David Parker asked why FIRST did not want to get involved in political issues. Jacques Schuurman replied that FIRST was strongly driven by US commercial interests who did not wish to be involved with governments, especially if there was a possibility of their involvement in information warfare.

6. Update on CHIHT

Andrew Cormack briefly reported on the CHIHT activity that was compiling a list of tools and guidelines for CSIRTs. The website (http://chiht.dfn-cert.de/) was starting to be used; the number of

visitors had doubled since the last TF-CSIRT meeting. It was planned to make a start with adding evaluations of tools.

Andy Bone commented that many of the tools were poorly documented, and this was an area where improvements could be made.

7. Update on Legal Handbook

Andrew Cormack reminded the meeting that the thinking about this issue actually pre-dated TF-CSIRT. When confronted with incidents intentionally caused by a person in a different country that are serious enough to wish to bring the person to justice, a CSIRT is faced with a lack of information: is the activity deployed illegal in the country concerned?, is it likely to be prosecuted there?, what evidence needs to be gathered?, who in law enforcement should be contacted? TF-CSIRT therefore developed the plan for a "handbook" for use by CSIRTs that would provide the answers to questions like this. More than two years ago TF-CSIRT suggested to the EC that the EC could play a useful role by commissioning such a handbook. For a long time nothing much happened, but last year the EC published a call for tender for this work, and a few days ago Andrew Cormack was contacted by the RAND Corporation who had won the bid. RAND will undertake the work as a six-months activity, to be completed by September 2003. A one-page project summary was distributed in the meeting.

RAND were now looking for input from TF-CSIRT members and had asked to distribute a questionnaire on the mailing list. In addition, they also proposed to hold a meeting in February with a few interested people from the Task Force. The meeting thought the questionnaire should be circulated as widely as possible.

ACTION 08-02. Andrew Cormack to circulate RAND questionnaire on the mailing list.

Tom Mullen thought that if RAND expected to collect information about legislation through this questionnaire it would be difficult for CSIRTs to answer the questions as it takes specialised lawyers to understand the law on these points.

Any persons interested to be involved in the work of RAND could contact them via Andrew Cormack by 31 January.

8. Results of seminar sessions

During the previous day's seminar, it had been agreed to form a working group on emergency backup infrastructures, comprising Gilles André, Kauto Huopio David Parker and John Wood. This group then met briefly and defined its charter as follows:
To identify in general terms, the potential threats to the European communications infrastructure. To identify alternative methods of communication that will enable information to be passed between CSIRTs with experiment as an objective.
The deliverable will be a proposal for an experiment.

The following presentations were suggested for the seminar sessions at the next TF-CSIRT meeting:

- Demonstration of tracker database – Andy Bone
- Demonstration of pilot implementation of IODEF – Jan Meijer
- CERT-RO – Vincent Thiele
- Assistance to the establishment of new CSIRTs – Przemek Jaroszewski
- Firewalls – Tomasz Nowocien and BT (contact Tom Mullen)

9. Responsible persons for Deliverables

The meeting agreed which persons would take responsibility for each of the work items listed in the TF-CSIRT Terms of Reference (see http://www.terena.nl/tech/task-forces/tf-csirt/TSec(02)017rev1-ToRTF-CSIRT.pdf). These persons were as follows:

A. Meetings, Seminars – Task Force chairman and secretary

B. Trusted Introducer – the members of the TI Review Board

C. Incident Description and Registration Framework – Jan Meijer, John Green, other eCSIRT.net participants

ACTION 08-03. Andy Bone to discuss with John Green his responsibility for work item C.

D. RIPE Database Security Object – Wilfried Wöber, Ulrich Kiermayr, Don Stikvoort

E. Clearing House for Incident handling Tools – Marco Thorbrügge, Andrew Cormack

F. Training of new (Staff of) CSIRTs – Andrew Cormack, Karel Vietsch

G. Assistance to the Establishment of new CSIRTs - Przemek Jaroszewski, Andrew Cormack

ACTION 08-04. Przemek Jaroszewski to report in the next TF-CSIRT meeting on the progress of work item G.

H. Incident Handling – Jan Meijer, Andy Bone, Kauto Huopio

ACTION 08-05. Jan Meijer to discuss the planning for work item H with Andy Bone and Kauto Huopio and to report in the next TF-CSIRT meeting.

I. Incident Information - David Parker, Andy Bone

David Parker had distributed a table showing different types of information with their sources, information sharing aspects, distribution restrictions and sensitivity duration. This provides a framework for exchanging information.

The next deliverable would now be to define specific areas on which CSIRTs would want to exchange information, and guidelines on how to do it. David Parker and Andy Bone undertook to expand the table to define the type of information that will be shared.

J. Collaboration with FIRST – to be reviewed in September 2003

After some discussion it was decided to review this work item in September 2003 after FIRST will have decided about its regionalisation effort.

Not yet in the official Terms of Reference:

K. Emergency backup infrastructure - Gilles André, Kauto Huopio David Parker, John Wood

10. Date of next meetings

The next meeting will be held on 29-30 May 2003 in Warsaw, Poland (hosted by CERT Polska / NASK). There will also be a TRANSITS training workshop (27-28 May 2003) and an EISPP workshop (28 May 2003) held in conjunction with this.

The following TF-CSIRT meeting will be hosted by CERT-NL in Amsterdam on 25-26 September 2003.

11. Any Other Business

Jacques Schuurman enquired about TF-CSIRT's contacts with the European Commission. Karel Vietsch reminded the meeting that over the past years TF-CSIRT deputations had regularly met with EC head of unit Thierry Van der Pyl and his collaborators (including Roman Tirler). Due to a current reorganisation of DG-InfoSoc, both Mr. Van der Pyl and Mr. Tirler were no longer in the same positions. The new head of unit was Mr. Gérald Santucci. It was agreed that it would be good to arrange a meeting with Mr. Santucci. Michel Miqueu, Andrew Cormack, Jacques Schuurman, David

Parker, Tom Mullen and possibly others would be interested to be part of the TF-CSIRT deputation at that meeting.

ACTION 08-06. Karel Vietsch to make an appointment for a meeting with Mr. Santucci, and ask on TF-CSIRT mailing list for participants in that meeting.

List of meeting participants

	Name	*Organisation*	*Country*
1.	Preben Andersen	DK-CERT	Denmark
2.	Gilles André	CERTA	France
3.	Jani Arnell	CERT-FI	Finland
4.	Matias Bevilacqua	esCERT-UPC	Spain
5.	Andy Bone	JANET-CERT	United Kingdom
6.	Cathy Booth	UNIRAS/NISCC	United Kingdom
7.	Gorazd Bozic (Chair)	SI-CERT	Slovenia
8.	Martin Camilleri	mtCERT	Malta
9.	Roberto Cecchini	GARR-CERT	Italy
10.	Garaidh Cochrane	JANET-CERT	United Kingdom
11.	Andrew Cormack	UKERNA	United Kingdom
12.	Michelle Danho	Renater CERT	France
13.	Aco Dmitrovic	SRCE	Croatia
14.	Michel Dupuy	CERTA	France
15.	Ralf Dörrie	Telekom-CERT	Germany
16.	Per Arne Enstad	Uninett CERT	Norway
17.	Mikhail Ganev	RU-CERT	Russia
18.	Rolf Gartmann	SWITCH-CERT	Switzerland
19.	Natasa Glavor	CARNet CERT	Croatia
20.	Pege Gustafsson	TeliaCERT	Sweden
21.	Kauto Huopio	CERT-FI	Finland
22.	Ulrich Kiermayr	ACOnet-IRT	Austria
23.	Pekka Kytölaakso	FUNET CERT	Finland
24.	Sergey Linde	RU-CERT	Russia
25.	Mirek Maj	CERT Polska	Poland
26.	Chelo Malagón	IRIS-CERT	Spain
27.	Miroslav Matijevic	CARNet CERT	Croatia
28.	Jan Meijer	SURFnet	The Netherlands
29.	Kevin Meynell (Secretary)	TERENA	-
30.	Michel Miqueu	CERT-IST	France
31.	Klaus Möller	DFN-CERT	Germany
32.	Francisco Monserrat	IRIS-CERT	Spain
33.	Tom Mullen	BTCERT	United Kingdom
34.	Tomasz Nowocien	POL34-CERT	Poland
35.	Joao Pagaime	FCCN	Portugal
36.	David Parker	UNIRAS/NISCC	United Kingdom
37.	Joan Ramon	esCERT-UPC	Spain
38.	Vlado Pribolsan	CARNet CERT	Croatia
39.	Maria Rådström	Telia Abuse	Sweden
40.	Jacques Schuurman	SURFnet	The Netherlands
41.	Harald Staub	SWITCH-CERT	Switzerland
42.	Don Stikvoort	Stelvio	The Netherlands
43.	Thomas Stridh	SUNET-CERT	Sweden
44.	Vincent Thiele	CERT-RO	The Netherlands
45.	Maris Urkis	LITNET CERT	Lithuania
46.	Karel Vietsch	TERENA	-
47.	Wilfried Wöber	ACOnet-IRT	Austria
48.	John Wood	MODCERT	United Kingdom

Apologies were received from:

Jimmy Arvidsson	TeliaCERT	Sweden
Damir Rajnovic	PSIRT	-

RESULTING ACTION ITEMS

05-07	Ian Bryant	Check NATO's interest in conducting special training and assisting the establishments of new CSIRTs in the EU and countries of the Former Soviet Union
07-03	Wilfried Wöber / TI	Produce documentation on how to use the IRT object in the RIPE database
07-07	all, Kevin Meynell	Send to Kevin Meynell URLs of projects that are relevant to CSIRTs, to be listed on the TF-CSIRT webpages
07-11	Don Stikvoort, BCP WG	Finalise Don Stikvoort's document on BCP in CSIRTs
07-12	BCP WG	Prepare presentation for managers
08-01	Karel Vietsch	Ensure that TRANSITS website is linked from TERENA website
08-02	Andrew Cormack	Circulate RAND questionnaire on TF-CSIRT mailing list
08-03	Andy Bone	Discuss with John Green his responsibility for work item C
08-04	Przemek Jaroszewski	Report in next TF-CSIRT meeting about the progress of work item G
08-05	Jan Meijer	Discuss the planning for work item H with Andy Bone and Kauto Huopio and report in the next TF-CSIRT meeting
08-06	Karel Vietsch	Make an appointment for a meeting with Mr. Santucci and ask on the TF-CSIRT mailing list for participants in that meeting