

**Minutes of the 11th TF-CSIRT meeting
Madrid, 16 January 2004**

[Please note that a seminar was held the previous day. Presentations from the seminar and the meeting can be found at <http://www.terena.nl/tech/task-forces/tf-csirt/meeting11/programmme.html>]

1. Welcome and apologies

Gorazd Bozic welcomed the participants. The list of those present and the list of people who sent their apologies are below at the end of these minutes.

He announced that the agenda items 5 and 11 would be swapped due to the schedule of the speakers.

2. Approval of the Minutes and Status of Actions from the last meeting

The minutes from the last meeting held on 26 September 2003 were approved.

Action items:

07-03 Wilfried Wöber/Ulrich Kiermayr - to produce the documentation on how to use the IRT object in the RIPE database.

Ongoing; see agenda item 9. A lot of documentation had been produced, therefore it was agreed to change the action to "maintain the documentation" and mark it as "ongoing".

07-11 Don Stikvoort and BCP WG - to finalise his document on the BCP in CSIRTs.

Done.

09-01. Jan Meijer - to create a questionnaire regarding the Incident Handling System requirements and send it to the mailing list.

Dropped. Jan Meijer explained that he had no time for this task and asked whether anyone else could take the initiative. Nobody volunteered and it was decided to drop the action.

09-11. Andrew Cormack and Przemek Jaroszewski - to initiate a discussion regarding ideas on how to involve more teams.

Done. Przemek Jaroszewski has sent an email to the TF-CSIRT mailing list, but received no replies. Karel Vietsch proposed to organise a small brainstorming meeting during the next TF-CSIRT meeting in Hamburg.

ACTION 11-01: Przemek Jaroszewski to organise a brainstorming meeting about involving new teams during the next TF-CSIRT meeting and to coordinate this meeting with Baiba Kaskina.

10-01 Klaus-Peter Kossakowski - to devise a proposal for the eCSIRT.net project follow-up, send it to the TF-CSIRT mailing list and lead the discussion about it in the next TF-CSIRT meeting.

Ongoing; Klaus-Peter Kossakowski had sent the proposal to the TI mailing list. The test phase of the follow-up project would be until end of March, the next proposal would be sent to the TI mailing list before the next TF-CSIRT meeting in Hamburg.

10-02 David Crochemore - to send information about the World Summit on Information Society to the TF-CSIRT mailing list.

Ongoing; Klaus-Peter Kossakowski said that David Crochemore was working on a draft, but it was not finalised yet. See agenda item 11.

10-03 Gorazd Bozic - to initiate a discussion on the TF-CSIRT mailing list on TF-CSIRT becoming a registered SIG of FIRST.

Ongoing; Gorazd Bozic promised to do this before the end of January.

10-04 Karel Vietsch - to contact Mr. Santucci and suggest having a meeting between the TF-CSIRT delegation and the EC in November 2003.

Done; see agenda item 6.

10-05 Marco Thorbrügge - to prepare the statistical information on the CHIHT website and present it in the next TF-CSIRT meeting.

Done; Marco Thorbrügge said that he had prepared not the statistical information, but the ideas for improvement. See agenda item 8.

10-06 Marco Thorbrügge - to include a sample CSIRT-workflow description as a prototype to the clearinghouse webpage and present it in the next TF-CSIRT meeting.

Done; see agenda item 8.

10-07 Gorazd Bozic - to finalise the new rules for participation in the TF-CSIRT and send them to the TF-CSIRT mailing list.

Done. Gorazd Bozic had sent the rules and since then he had been using them to decide about the subscription to the TF-CSIRT mailing list.

10-08 Jan Meijer - to prepare a charter and list of deliverables for the IODEF exchange protocol working group and present them in the next TF-CSIRT meeting.

Done; see agenda item 12.

10-09 Ian Bryant - to prepare a charter and list of deliverables for the working group on a possible unified Vulnerability and Exploit Description and Exchange Format and present them in the next TF-CSIRT meeting.

Done; see agenda item 10.

3. Trusted Introducer Service

3.1. Status Report and feedback from the meeting of accredited CSIRTs

Don Stikvoort presented the TI status report and feedback from the meeting of accredited CSIRTs that was held on the previous day. He emphasised the importance of building the trust network and the means that the TI uses for that, i.e. the accreditation process. The TI database contains data on listed teams and accredited teams. He also presented charts with the number of CSIRTs in the TI repository and accredited CSIRTs.

The accredited teams were considering adding a “Code of Ethics” to the accreditation requirements. Gilles André asked whether the “Code of Ethics” would be public. Don Stikvoort replied that it would become available when teams reached the consensus.

Don Stikvoort named the TI team members and thanked for the trust of the community.

3.2. Report from the TI Review Board

Karel Vietsch reported on the meeting of the TI Review Board that was held on the previous day. He explained the role of the TI Review Board and mentioned the main topics of discussion.

The TI Review Board reviewed the TI accredited teams meeting, particularly the “code of Ethics” discussion. In spite of fact that consensus was not reached, it should be considered as an important topic for further work.

The outcome of the eCSIRT.net project was discussed, see agenda item 4.1. Don Stikvoort presented a more detailed status update of the TI.

The dialogue with FIRST was discussed as well; the issue was presented by Klaus-Peter Kossakowski and Udo Schweigert. The question was raised whether FIRST could use for their own business the list of criteria used by the TI. As the list of criteria is public, there were no objections.

Karel Vietsch summarised that the meeting of accredited CSIRTs was very positive with a very appropriate intensity of discussions. He thanked the TI team.

The next meeting of the accredited CSIRTs and the next TI Review Board meeting will be held in Hamburg, adjacent to the next TF-CSIRT meeting.

4. Update on the EC funded projects

4.1. eCSIRT.net

Klaus-Peter Kossakowski reported on the eCSIRT.net project, which aims to develop a standardised way for exchanging incident-related information. His presentation addressed the project perspective, results for the IDS related activities and the workshop on early warning.

The project has formally ended on 31 December 2003, the final review would be in February 2004, and afterwards the results would be available on-line. Based on these results the eCSIRT.net team would define areas of interest and prepare a proposal for the TI accredited teams meeting in Hamburg on how to proceed. Results of the project should be discussed in that meeting.

Klaus-Peter Kossakowski presented results for the IDS related activities with the problem statement, observations and graphs. He paid special attention to the criteria for splitting the unknown traffic.

Summarising the experiences gained, he proposed to organise a workshop about early warning issues and to share experience and opinions. The workshop should focus on discussions rather than on presentations. The workshop will be held in conjunction with the next TF-CSIRT meeting in Hamburg. Klaus-Peter Kossakowski will organise the workshop and send the information to the TF-CSIRT mailing list.

ACTION 11-02: Klaus-Peter Kossakowski - to organise a workshop on early warning in conjunction with the next TF-CSIRT meeting in Hamburg and send the information about it to the TF-CSIRT mailing list.

4.2. EISPP

Udo Schweigert gave a short report on the EISPP project. The project ended in January 2004. The project's objective was to organise CERT cooperation on security advisories. He mentioned briefly the motivation and work process in the project.

The results of the EISPP project, relevant for improving the CERT cooperation on vulnerability handling and advisory creating, were a common advisory format and roadmap for establishing CEISNE (Co-operative European Information Security Network of Expertise). Regarding the common advisory format Udo Schweigert emphasised that version 1.2 was available and version 1.3 was expected by the end of January 2004. He encouraged everyone to read about it in more detail on-line (the URL was provided in the presentation).

He said that this format was used by at least 3 CERTs in Germany, as well as in France and Italy. The common advisory format was the only format used in more than one country. Udo Schweigert proposed to all who might be interested in using the format to join the working group. He would provide more details upon request by email.

4.3. TRANSITS

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

The project is contracted to produce the 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). Karel Vietsch gave some details about the trainees from the first three workshops. He mentioned that more students from governmental and commercial sectors would be welcome.

The TRANSITS project had been reviewed in Brussels on 15 December 2003, with a very positive result. Andrew Cormack has been working on the revision of the training materials, the new version

should be completed before March 2004. The 4th TRANSITS workshop will be held near Hamburg before the 12th TF-CSIRT meeting in May 2004.

Marco Thorbrügge asked what feedback would be expected from those who use the TRANSITS materials for other trainings. Karel Vietsch replied that TERENA uses an evaluation form to get the feedback, but from the others feedback in any format would be very valuable. Gorazd Bozic proposed to put the evaluation form on-line, so that others could use it as well. Karel Vietsch promised to consider this proposal.

Gilles André asked about the possible plans for continuation of the project. Karel Vietsch said that the EC is looking for projects from the CERT community, so it would be possible to create a proposal as a follow-up of the TRANSITS project, maybe together with some follow-up of the eCSIRT.net and EISPP projects. Another possibility would be to organise courses on a self-funded basis. Both possibilities should be considered in the future.

5. Update on Abuse forum meeting

Pege Gustafsson presented information about the Abuse forum meeting which was held on Wednesday before the TF-CSIRT seminar. He outlined the organisers of the meeting, the type of audience they had, and all kinds of problems they are dealing with. There were 27 participants from different sectors in the Abuse forum meeting.

The main conclusion of the meeting was that Abuse teams share similar problems and cooperation would be much needed. They would like to form a sub-group under the umbrella of TF-CSIRT. The first milestones would be to write the proposed guidelines for abuse team work and to organise the next workshop in conjunction with the next TF-CSIRT meeting in Hamburg.

After the presentation it was discussed whether TF-CSIRT would want to adopt the Abuse forum as one of its sub-groups and whether the members of the Abuse group should mandatory become TF-CSIRT members. People expressed various opinions and doubts whether TF-CSIRT would need a sub-group whose members would not be members of TF-CSIRT. Some people doubted whether Abuse teams and CSIRT teams were so different that a need for a separate forum would be justified. Pege Gustafsson insisted that there were some overlaps in the problems, but the Abuse teams in general were dealing with different issues and worked more closely with the end users than the CSIRT teams. Therefore a separate forum would be needed.

Gorazd Bozic summarised the discussion and proposed to Pege Gustafsson not to take any definite decisions but instead go step by step. The first steps would be the document describing the planned activities of the Abuse forum and the next workshop together with the TF-CSIRT meeting. Both groups would stay separately and work in cooperation particularly on the topics which overlap. He thought that after the next Abuse forum workshop it could be easier to justify whether closer cooperation would be needed or not.

ACTION 11-03: Pege Gustafsson – to draft the document about the planned activities of the Abuse forum before the next TF-CSIRT meeting.

Pege Gustafsson also asked whether TERENA could host the website and mailinglist for the Abuse forum. It was agreed to postpone this question until consensus about the future cooperation between the groups would be achieved.

6. Update on contacts with European Commission (including ENISA)

Karel Vietsch reminded the participants about the meeting with the EC which was held in November and Gorazd Bozic reported about the latest developments regarding ENISA.

Karel Vietsch gave an overview on the meeting with the EC officials held on 11 November 2003 in Brussels. He had sent a report about the meeting to the TF-CSIRT mailing list, therefore just the main points were briefly repeated, i.e. the preparation of ENISA, the possible follow-up of current FP5 projects, the legal handbook issue, the eTEN programme. He emphasised that the EC would be willing to see more project proposals from CSIRTs submitted in the next call, which will be early in 2005. In

the year until then, the Commission officials would like to work closely with the CSIRT community so that the contents of the call for proposals would address the priority topics of that community.

The MODINIS programme was mentioned as a possibility for the EC to sponsor the FIRST conference 2004 in Budapest. However, Klaus-Peter Kossakowski added that no decision about the sponsorship has been taken yet.

The question was raised whether the Legal Handbook would be available electronically. Karel Vietsch replied that that was promised by the EC officials and in January 2004 it has already become available.

The next meeting with the EC officials could be organised before the summer 2004. The main topic of that meeting would be how the CSIRT community would like to influence the next call for project proposals in early 2005. Karel Vietsch encouraged everyone to think about that and send all ideas to him.

Gorazd Bozic continued the topic with a report from the meeting of the Inter-Disciplinary Working Group (IDWG) that is advising on the establishment of ENISA. The meeting was held on 12 December 2003 in Brussels. He said that he was pleasantly surprised by the outcome of the meeting. A report about this meeting has been sent to the TF-CSIRT mailing list by Andrew Cormack.

Gorazd Bozic pointed out the main issues mentioned in the meeting, i.e. legal aspects regarding the creation of the Agency, recruitment of the executive director and other staff, formation of the management board, the programme of the Agency. The EC has decided that ENISA will be located in Greece. Gorazd Bozic also mentioned the proposal to hire an outside expert for 6 months to help with the establishment of the Agency.

The EC was planning to organise a workshop in 2006 to explain the mission and activities of the ENISA. Before then the Agency should be established.

The CSIRT community is represented in the IDWG by Gorazd Bozic, Andrew Cormack and Martin Camilleri. All ENSIA related questions and issues could be addressed to them. Gorazd Bozic promised to keep the TF-CSIRT community informed about the latest developments regarding the Agency.

7. Presentation/discussion on the European Government CERTs

David Parker gave a presentation about the European Government CSIRTs (EGC). The aim of the presentation was to clarify relations between the EGC and TF-CSIRT and to inform the participants about the activities of the EGC.

David Parker outlined the history of the EGC and the related technical working group (WG). This WG was dealing with the incidents affecting government and new vulnerabilities. The EGC was meeting once every four months and has expanded to 6 countries since the year 2002. The EGC has become more formal with a "Mutual Agreement of Scope", but still could be considered as an informal group with a technical focus.

The scope and goals of the EGC were mentioned. Regarding the relationship with TF-CSIRT, David Parker mentioned that the EGC supported TF-CSIRT and other CSIRT activities in Europe, the EGC teams were members of TF-CSIRT, and the EGC recognised TF-CSIRT's role in establishing cooperation among CSIRTs in Europe, developing technical CSIRT initiatives and collaborative projects.

As the achievements of the EGC David Parker noted the established trusted relationships that allowed the exchange of government sensitive material in relation to incidents, the cooperative working relationships in relation to vulnerability research programs, and the set-up of a government-level alerting system to combat electronic attack incidents.

David Parker spoke about the future goals of the EGC, including support for the activities of TF-CSIRT, i.e. information sharing, assisting the group with EGC experience and expertise, promotion of the TF-CSIRT views. Other future activities he mentioned were to develop the capabilities of the EGC group in relation to the government-level incident response, to enhance current alerting system, to

increase the level of cooperation in relation to vulnerability research and disclosure, to support the activities of ENISA and similar initiatives.

Jacques Schuurman asked about the point of view of the EGC on FIRST. David Parker replied that all the EGC teams are members of FIRST, but they have not discussed a common view.

Damir Rajnovic wanted to know whether the EGC have thought about a single point of contact for Europe, as an example APCERT for Asia was mentioned. Karel Vietsch thought that Europe was too developed to have one single point of contact. It would not be possible even to define a single point of contact for each country. Damir Rajnovic specified that he meant this point of contact for information purposes. David Parker replied that for information purposes the EGC WG could be used. Doug Pearson asked what type of mechanism was used for information sharing. David Parker replied that usually it was electronic exchange of information, but in the urgent matters the TI list with phone numbers could be used.

8. Improvements to CHIHT

Marco Thorbrügge spoke about the possible enhancement of the clearing house service. He mentioned the history of CHIHT and presented the possibilities for the future, i.e. to leave it as it was, to re-discuss the structure of CHIHT, to start a new poll, to add some additional value to the project.

In the existing version of CHIHT all the tools were in one level, Marco Thorbrügge proposed to categorise them and to add extra value to the project. He showed an example of workflow for the incident report about the root compromise. By clicking on a particular box in the workflow scheme it was possible to get information about the relevant tools.

As future tasks for CHIHT Marco Thorbrügge identified collecting and generating basic workflows, starting a new survey, and discussing a standard format for workflow-graphics. He asked for the audience's opinion.

The feedback from the group was very positive. Marco Thorbrügge proposed to summarise his ideas and send them to the TF-CSIRT mailing list. He also asked for volunteers to help him with CHIHT development, 2 people would be enough. Rolf Gartmann from SWITCH volunteered.

ACTION 11-04: Marco Thorbrügge – to summarise proposals about the future of CHIHT and send them to the TF-CSIRT mailing list.

Wilfried Wöber asked whether any relationship between CHIHT and TRANSITS training materials existed. Marco Thorbrügge replied that no relation existed, these materials were not connected. Suleyman Anil asked who would be maintaining the material. Marco Thorbrügge replied that it would be his task together with Rolf Gartmann. Jacques Schuurman offered his help by sending the relevant information from SURFnet's repository.

ACTION 11-05: Jacques Schuurman – to send the information related to CHIHT from SURFnet's repository.

Jacques Schuurman raised the issue who would be eligible to access the CHIHT information. Marco Thorbrügge replied that so far all the information has been open to everyone and it would be up to TF-CSIRT people to decide for the future.

In conclusion Marco Thorbrügge agreed to produce a new survey about the tools and to present the latest developments of CHIHT in the next TF-CSIRT meeting.

ACTION 11-06: Marco Thorbrügge – to produce a new survey about the tools for CHIHT and to present latest developments of CHIHT in the next TF-CSIRT meeting.

9. Update on IRT object issues and WG

Wilfried Wöber reported about the recent developments regarding the IRT object and working group (WG). The documentation about the IRT object has been compiled and extended; some teams have

tagged all the address objects of their constituency. A discussion has sprung up on the RIPE DB-WG mailing list about complexity of the IRT object and possible simplifications. Wilfried Wöber encouraged people to participate in this discussion.

He also mentioned the invitation from the APCERT community to go to the APRICOT conference in Kuala Lumpur, in February 2004 and report about the IRT object. Wilfried Wöber asked whether the TF-CSIRT community would support this presentation. The feedback was very positive.

Wilfried Wöber said that according to the latest information, the ARIN database has had a functionality similar to the IRT object for long time and it has been used as an AbuseORG object. It has not been decided yet how to use this functionality for information or data exchange.

Gorazd Bozic summarised that the group highly supported Wilfried Wöber's mission to Malaysia and would hope to hear a report about it in the next TF-CSIRT meeting.

10. Update on Vulnerability and Exploit Description and Exchange Format (VEDEF) WG

Ian Bryant gave an overview of the activities of the VEDEF WG. He started his presentation with information about the National Infrastructure Security Coordination Centre (NISCC), its structure and activities. He mentioned the current initiatives regarding description and exchange formats (DEFs), including the intrusion detection DEF, the incident object DEF, the penetration testing DEF, and the vulnerability and exploit DEF. In relation to the last one, it has been proposed to form a TF-CSIRT working group.

Ian Bryant presented a more detailed overview on the VEDEF history, needs, initiatives, and basic information requirements. Regarding the latest initiatives he mentioned EISPP, RUSCERT, OpenSec, and OASIS. In some of them the TF-CSIRT community had participated.

This presentation was prepared as a formal proposal for creating the working group. The draft charter of the WG has been circulated to the TF-CSIRT mailing list already. The final charter should be ready by 31 January 2004. Ian Bryant informed the meeting about organisational aspects of the WG and possible outputs. He also paid attention to the deliverables of the WG.

Jan Meijer proposed to establish this working group through IETF, because that would secure the support from vendors. Ian Bryant said that he had already contacted some vendors regarding their support.

Damir Rajnovic asked about the relation with the EISPP project. Ian Bryant replied that the VEDEF WG would directly pick up and run the EISPP job. No further questions were raised. The meeting expressed its support to this initiative.

11. Update on FIRST

Klaus-Peter Kossakowski and Udo Schweigert reported about the latest activities in FIRST. Klaus-Peter Kossakowski spoke about the World Summit on Information Society (WSIS) which took place in Geneva in December 2003. He mentioned that FIRST participated there as a non-governmental organisation. As the main issues from the WSIS he noted privacy and legal aspects. The next World Summit will be held in Tunis in November 2005 and FIRST would like to have more influence there.

Udo Schweigert reported on the FIRST SC (Steering Committee) face-to-face meeting which was held in New York. The meeting focused mainly on strategical issues, they thought that FIRST should become more a "members do" organisation. The reason for problems with FIRST and lack of activity from membership could be related to trust. Therefore a new trust model would be needed. For that a new membership committee has been established with about 15 members and they would try to investigate the situation and find solutions. The committee would like to use the TI approach; the TI Review Board would be involved in these discussions.

The FIRST SC has decided to introduce two awards – one for a member and one for a vendor. The criteria have not been set yet. This should assess the willingness within the membership.

Andy Bone noted that maybe FIRST's major problem was its size. Udo Schweigert replied that it was definitely an issue and probably a regional organisation scheme would work better. It would be better to have "people do" type of working groups, than "team/member do" ones. He admitted that this issue should be addressed.

The next FIRST conference will be held in Budapest in June 2004. Udo Schweigert encouraged as many people as possible to come. The registration should be open by mid February 2004, certainly after the Technical Colloquium (TC) in San Jose (California).

FIRST was considering to use the TRANSITS's course materials for its newly established members, e.g. from Latin America. The plan would be to train trainees from the FIRST community and encourage them to organise courses for the local communities. FIRST has been discussing that with APCERT already. Karel Vietsch remarked that for the TRANSITS course the language might be a problem. For example, in Latin America Spanish should be used instead of English. He mentioned that even with its current geographical scope TRANSITS had found language to be a problem. Udo Schweigert agreed that it was an issue and said that FIRST would support local trainees as much as possible.

Gilles André asked whether FIRST would be using exactly the TI documentation and materials or they would be adapted. Udo Schweigert said that materials would be adapted considering FIRST needs and specifics.

12. Update on IODEF

Jan Meijer presented the latest developments of IODEF, including the overview, the status of INCH, usage cases and hints. He paid special attention to the current activities, i.e. building an authoritative source for the eCSIRT.net IODEF profile and common language, implementing an IODEF exchange protocol, offering support for the current IODEF-exchange network, assisting the TF-CSIRT teams that would like to join the IODEF-exchange network, promoting the implementation of IODEF in other forums.

The deliverables would be a working demo -bed for the exchange protocol, protocol documentation, related HOWTO and FAQ documents, a standard web form package for reporting incidents that output IODEF, and a 2-hour workshop on implementation, which could be held in May or September 2004.

Jan Meijer also mentioned the proposal for another working group, i.e. Building Blocks for IODEF Exchange Network WG (BIEN WG). This working group would work on enabling the exchange of incident-related information between incompatible incident handling systems of different CSIRTs in different administrative domains. The ultimate goal would be to automate the exchange of incident-related information (data and meta-data) between incident handling systems as much as possible without human intervention.

The working group itself was small (2-3 people), in the future it would continue reporting to TF-CSIRT on the mailing list and in the meetings. Fully involved people were Jan Meijer and John Green. Jan Meijer also promised to forward all the interesting information regarding the IODEF developments to the TF-CSIRT mailing list.

13. TF-CSIRT liaison with GN2 JRA2

Jacques Schuurman, Karel Vietsch and Robert Walton informed the audience about the GN2 project proposal, the second joint research activity (JRA2) and its liaison with TF-CSIRT.

GN2 is a follow-up project of Geant, the project proposal has been submitted to the EC and it has passed the first evaluation phase positively. The possible start date for the project could be 1 September 2004. The project proposal contained 5 joint research activities, the second (JRA2) was named "Security". The total proposed budget of JRA2 was 55 man-years and the contribution asked from the EC was about 1 million EUR. The duration of the GN2 project would be 4-5 years. In JRA2, TF-CSIRT had been mentioned as one of the key-players with an advisory role. TF-CSIRT was expected to cooperate with JRA2 involved people and contribute to particular tasks. Therefore the community should discuss the possible cooperation.

Gorazd Bozic read the bullet points from the proposal about the cooperation, i.e. information exchange, JRA2 presentations in the TF-CSIRT meetings, advisory role, joint and side-by-side meetings. He promised to circulate all the relevant documents to the mailing list.

ACTION 11-07: Gorazd Bozic - to circulate GN2 JRA2 related relevant documents to the TF-CSIRT mailing list.

Jacques Schuurman said that he and a few other people from the TF-CSIRT community were involved in the working group which worked on specifying the JRA2 part in the GN2 project contract, including the goals, deliverables and milestones. The working group has to specify activities, to distribute the available resources and to find the NRENs to do the defined tasks. It was asked who were participating in the working group. Jacques Schuurman replied that all European NRENs had been invited to appoint their security experts as members of that group.

The current version of the proposal was too immature to send to the mailing list, but it would be possible to distribute the proposal when it would be finished. Christoph Graf was the leader of the working group, so he could present the contents of the GN2 JRA2 plans in the next TF-CSIRT meeting.

14. Results of the seminar sessions, ideas for the future sessions

Gorazd Bozic asked the group for feedback about the yesterday's seminar sessions and reminded them to fill in the evaluation forms. Jan Meijer said that it would be very significant to ask Simon Contant from Microsoft to come to the next TF-CSIRT seminar and present his topic. Baiba Kaskina replied that Simon Contant already offered this possibility, so hopefully he would give the presentation during the next TF-CSIRT seminar.

15. Status of the other TF-CSIRT work items / deliverables

Gorazd Bozic proposed to go through the work items and review their status. As the mandate of TF-CSIRT will expire in May 2004, new Terms of Reference (ToR) would be needed.

About the work items A, B, C, and D no comments were made, these items were on track and developing positively. Regarding work item E it was noted that possible developments had been discussed (see agenda item 8). Work item F – the TRANSITS courses have been organised and new staff has been trained. Work item G – no ongoing activities, but Przemyslaw Jaroszewski would initiate a new brainstorming meeting (see action item 11-01). It was agreed to drop work item H (see agenda item 2, action 09-01), so it should be removed from the next ToR. The continuation of the work item I would be related to the follow-up of the eCSIRT.net project.

Regarding the last action item (J, Collaboration with FIRST) a discussion arose. Andy Bone asked whether anyone would present the TF-CSIRT activities in the next FIRST conference. Damir Rajnovic supported this idea and thought that it should be an ongoing task. Gorazd Bozic agreed that it would be a very good idea and it would be best to have a fixed slot in the main conference programme for reports from the Regional Initiatives (RI). But he doubted if it would be possible to get a slot for this year's conference. Karel Vietsch opposed saying that FIRST has expressed their interest about the activities of TF-CSIRT, so they should find a place and time for the presentation. Andy Bone agreed that TF-CSIRT should inform the FIRST community about their activities every year.

Don Stikvoort proposed to contact the FIRST secretariat regarding the possibilities to present TF-CSIRT in this year's conference. Gorazd Bozic agreed to draft a formal request and contact the FIRST secretariat.

ACTION 11-08: Gorazd Bozic – to contact the FIRST secretariat regarding the possibility to present the TF-CSIRT activities in the FIRST conference 2004.

Gorazd Bozic suggested that APCERT should be contacted as well about the possible joint presentation or shared slot in the conference. David Parker agreed to contact Graham Ingram from APCERT regarding this issue.

ACTION 11-09: David Parker – to contact APCERT people regarding the possible joint presentation or shared slot in the FIRST conference 2004.

Gorazd Bozic summarised the status of work items. Work item H should be dropped, some items should be reformulated. Karel Vietsch proposed that Baiba Kaskina would contact all the leaders of the work items and agree on new formulations for the new ToR. That should be done before the next TF-CSIRT meeting. He also noted that some new work items should be added, e.g. RTIR WG VEDEF WG and BIEN WG activities.

ACTION 11-10: Baiba Kaskina – to contact all the leaders of the work items and agree about the new formulation of the work item for the new version of the TF-CSIRT ToR.

Karel Vietsch asked everyone to send their ideas about new work items for the new ToR of TF-CSIRT to the mailing list.

Andy Bone asked whether the “Code of Ethics” should be added as a work item. Gorazd Bozic thought that it was not mature enough to include in the ToR and should be worked on firstly within the smaller community of accredited CSIRTs.

16. Date of the next meetings

The next meeting will be held on 27-28 May 2004 in Hamburg, Germany (hosted by DFN-CERT).

The subsequent TF-CSIRT meeting will be hosted by mtCERT in Malta on 23-24 September 2004.

Gorazd Bozic asked who could host the following meeting in January 2005. Andy Bone said that it could be JANET-CERT and the location could be London, but he should check if it would be feasible for JANET and if the location would be available.

17. Any Other Business

The meeting expressed its thanks to IRIS-CERT, RedIRIS and the Universidad Complutense for organising a great meeting.

List of meeting participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
1. Preben Andersen	DK-CERT	Denmark
2. Gilles André	CERTA	France
3. Suleyman Anil	NATO (NCIRC)	Belgium
4. Jani Arnell	FICORA / CERT-FI	Finland
5. Pär Österberg	SITIC	Sweden
6. Andy Bone	JANET-CERT	United Kingdom
7. Gorazd Bozic (Chair)	SI-CERT	Slovenia
8. Ian Bryant	NISCC R&D	United Kingdom
9. Martin Camilleri	mtCERT	Malta
10. Roberto Cecchini	GARR-CERT	Italy
11. Garaidh Cochrane	JANET-CERT	United Kingdom
12. José Enrique Díaz Jiménez	NATO (NCIRC)	Belgium
13. Ralf Dörrie	Telekom-CERT	Germany
14. Erik de Jong	GOVCERT.NL	The Netherlands
15. Gary Dooley	Royal Mail Group	United Kingdom
16. Michel Dupuy	CERTA	France
17. Øyvind Eilertsen	UNINETT CERT	Norway
18. Lionel Ferette	BELNET	Belgium
19. Carles Frago	CESCA-ERAC	Spain
20. Carlos Fuentes	IRIS-CERT, RedIRIS	Spain
21. Manuel Garcia-Cervigon	esCERT-UPC	Spain
22. Rolf Gartmann	SWITCH	Switzerland

23. Gema Gómez	esCERT-UPC	Spain
24. Natasa Glavor	CARNet	Croatia
25. John Green	JANET-CERT	United Kingdom
26. Christine Greenhalgh	BT SBS	United Kingdom
27. Jon Grew	BT SBS	United Kingdom
28. Pege Gustafsson	TeliaCERT	Sweden
29. Peter Haag	SWITCH-CERT	Switzerland
30. Kauto Huopio	FICORA / CERT-FI	Finland
31. Przemyslaw Jaroszewski	CERT Polska / NASK	Poland
32. Stephane Kardas	CERTA	France
33. Baiba Kaskina (Secretary)	TERENA	-
34. Ulrich Kiermayr	ACOnet-IRT	Austria
35. Klaus-Peter Kossakowski	PRESECURE	Germany
36. Pekka Kytölaakso	FUNET Cert	Finland
37. Mirosław Maj	CERT Polska	Poland
38. Chelo Malagón	IRIS-CERT, RedIRIS	Spain
39. Johan Martensson	SITIC	Sweden
40. Jan Meijer	SURFnet / CERT-NL	The Netherlands
41. Janos Mohacsi	NIIF/HUNGARNET	Hungary
42. Francisco Jesus Monserrat Coll	IRIS-CERT, RedIRIS	Spain
43. Tassos Moschos	GRNET-CERT	Greece
44. Gustavo Neves	FCCN (CERT.PT)	Portugal
45. Tomasz Nowocien	POL34-CERT	Poland
46. Carol Overes	GOVCERT.NL	The Netherlands
47. João Pagaiame	FCCN (CERT.PT)	Portugal
48. David Parker	UNIRAS/NISCC	United Kingdom
49. Doug Pearson	Indiana University	USA
50. Peter Quick	Telekom-CERT / T-Com	Germany
51. Damir Rajnovic	Cisco Systems	United Kingdom
52. Maria Rådström	Telia Abuse	Sweden
53. Jacques Schuurman	SURFnet / CERT-NL	The Netherlands
54. Udo Schweigert	Siemens CERT	Germany
55. Mikel Stamm	DK-CERT	Denmark
56. Don Stikvoort	Trusted Introducer	The Netherlands
57. Marco Thorbrügge	DFN-CERT	Germany
58. Maris Urkis	LITNET CERT	Lithuania
59. Hedy van der Ende	GOVCERT.NL	The Netherlands
60. Karel Vietsch	TERENA	-
61. Robert Walton	DANTE (Dancert)	United Kingdom
62. Torbjörn Wictorin	SUNet-CERT	Sweden
63. Wilfried Wöber	ACOnet-IRT	Austria
64. Jörg Zemke	Philips	The Netherlands

Apologies were received from:

Jimmy Arvidsson	TeliaCERT	Sweden
Andrew Cormack	UKERNA	United Kingdom
Jan Droemer	Philips	the Netherlands
Mikhail Ganev	RU-CERT	Russia
Sergey Linde	RU-CERT	Russia
Stelios Maistros	GRNET-CERT	Greece
Vlado Pribolsan	CARNet CERT	Croatia
Gareth Price	BT SBS	United Kingdom

RESULTING ACTION ITEMS

07-03	Wilfried Wöber/ Ulrich Kiermayr	Maintain the documentation on how to use the IRT object in the RIPE database.
10-01	Klaus-Peter Kossakowski	Devise a proposal for the eCSIRT.net project follow-up, send it to the TI mailing list and lead the discussion about it in the next TI accredited teams meeting.
10-02	David Crochemore	Send information about the World Summit on Information Society to the TF-CSIRT mailing list.
10-03	Gorazd Bozic	Initiate a discussion on the TF-CSIRT mailing list on TF-CSIRT becoming a registered SIG of FIRST.
11-01	Przemek Jaroszewski	Organise a brainstorming meeting about involving new teams during the next TF-CSIRT meeting and to coordinate this meeting with Baiba Kaskina.
11-02	Klaus-Peter Kossakowski	Organise a workshop on early warning in conjunction with the next TF-CSIRT meeting in Hamburg and send the information about it to the TF-CSIRT mailing list.
11-03	Pege Gustafsson	Draft the document about the planned activities of the Abuse forum before the next TF-CSIRT meeting.
11-04	Marco Thorbrügge	Summarise proposals about the future of CHIHT and send them to the TF-CSIRT mailing list.
11-05	Jacques Schuurman	Send the information related to CHIHT from SURFnet's repository.
11-06	Marco Thorbrügge	Produce a new survey about the tools for CHIHT and present latest developments of CHIHT in the next TF-CSIRT meeting.
11-07	Gorazd Bozic	Circulate GN2 JRA2 related relevant documents to the TF-CSIRT mailing list.
11-08	Gorazd Bozic	Contact the FIRST secretariat regarding the possibility to present the TF-CSIRT activities in the FIRST conference 2004.
11-09	David Parker	Contact APCERT people regarding the possible joint presentation or shared slot in the FIRST conference 2004.
11-10	Baiba Kaskina	Contact all the leaders of the work items and agree about the new formulation of the work item for the new version of the TF-CSIRT ToR.