TSec(04)096

Minutes of the 12th TF-CSIRT meeting
Hamburg, 28 May 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/meeting12/programme.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.

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

The minutes from the last meeting held on 16 January 2004 were approved.

Action items:

07-03 Wilfried Wöber/ Ulrich Kiermayr – to maintain the documentation on how to use the IRT object in the RIPE database.
Ongoing; see agenda item 8. The documentation is on the TI and RIPE-NCC websites, it would be maintained further.

10-01 Klaus-Peter Kossakowski – to 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.
Done. It has been addressed in the TI accredited teams meeting which was held on the day before the TF-CSIRT meeting.

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

10-03 Gorazd Bozic – to initiate a discussion on the TF-CSIRT mailing list on TF-CSIRT becoming a registered SIG of FIRST.
Dropped. Gorazd Bozic has not done it because of the discussion in the TF-CSIRT mailing list in late 2003. The main concern was asymmetry which would occur if TF-CSIRT would become a SIG. Gorazd Bozic asked whether anyone thought that TF-CSIRT should become a SIG. As no one did, the action was dropped.

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.
Dropped. Przemek Jaroszewski explained that this topic has been discussed with Andrew Cormack and Baiba Kaskina and there would be changes in the new Terms of Reference, but no BoF would be organised.

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.
Done, the workshop was successful.

11-03 Pege Gustafsson – to draft the document about the planned activities of the Abuse forum before the next TF-CSIRT meeting.
Done. Peter Quick explained that short notes with future steps for the Abuse forum and a presentation for the Abuse workshop have been produced.

11-04 Marco Thorbrügge – to summarise proposals about the future of CHIHT and send them to the TF-CSIRT mailing list.
Done; see agenda item 7.

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

11-06 Marco Thorbrügge – to produce a new survey about the tools for CHIHT and present latest developments of CHIHT in the next TF-CSIRT meeting.
Ongoing; see agenda item 7.

11-07 Gorazd Bozic – to circulate GN2 JRA2 related relevant documents to the TF-CSIRT mailing list.
Ongoing. Christoph Graf has taken over this action. The document has not been circulated because negotiations with the EC were still ongoing. Some information about the JRA2 has been sent to the TF-CSIRT mailing list. The documents could be circulated in September 2004.

11-08 Gorazd Bozic – to contact the FIRST secretariat regarding the possibility to present the TF-CSIRT activities in the FIRST conference 2004.
Done. The paper has been accepted and there would be a presentation about TF-CSIRT during the FIRST conference. It would be in the same slot with the Asia-Pacific CERT presentation.

11-09 David Parker – to contact APCERT people regarding the possible joint presentation or shared slot in the FIRST conference 2004.
Done. It has been discussed to have such presentations in the FIRST conference regularly.

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.
Done; see agenda item 14.

3. Trusted Introducer Service

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

Antonio Liu presented the TI status report and feedback from the meeting of accredited CSIRTs that was held on the previous day. He presented charts with the number of CSIRTs in the TI repository and accredited CSIRTs.

The accredited teams have discussed three major topics, i.e. IRT object, Code of Conduct, new TI services.

IRT object has gained acceptance in Europe, about 7.1% of the RIPE IP address space were connected to an IRT object. Wilfried Wöber and Don Stikvoort would present the IRT object at the FIRST Conference 2004 in Budapest.

Antonio Liu named the authors of the new draft of the Code of Conduct. The draft has been discussed and the new version would be circulated.

The new TI services were presented as well, including the eCSIRT.net pilot project results, the security repository for collection and representation of common data, the authentic and confidential transmission of email via a re-encrypting mail gateway.

3.2. Report from the TI Review Board

Karel Vietsch reported on the meeting of the TI Review Board (TI RB) that was held on the previous day. He explained the role of the TI Review Board and mentioned the main topics of discussion. Jimmy Ardvidsson's term in the TI RB would expire in September 2004 and elections would take place in Malta.

The agenda of the TI RB meeting was very similar to the TI accredited teams meeting. The TI RB in the future would report only to the TI accredited teams, not to the whole TF-CSIRT.

The TI RB reviewed the TI accredited teams meeting, particularly the Code of Conduct discussion. Main difficulties to agree on the Code of Conduct are due to language and cultural differences. Initially

such a Code should be in the form of recommendations and not be a condition for accreditation, otherwise its implementation would be impossible. Later, after some experience had been gained and after amendments as required, the Code of Conduct could possibly become compulsory for the accredited teams. The concept of the "sub-CSIRT" and the new services were discussed as well.

Karel Vietsch summarised that the meeting of accredited CSIRTs was constructive, but it required much better preparation. Documentation should be available sooner and be more mature and each agenda item should be presented with slides. The chair of the TI RB would be involved in the preparation of the agenda and meeting documents in the future.

The TI RB meeting also has discussed the last TI Status Report, possible rearrangement of the contract between TERENA and S-CURE, the case of non-paying accredited CSIRT, and the preparation of the annual review of the TI services. Information about (non-)payment should be better coordinated between TERENA and S-CURE. The agreement between TERENA and S-CURE should be changed to an agreement between TERENA and a consortium existing of PRESECURE and S-CURE to avoid S-CURE being the single point of failure. Don Stikvoort would consider such agreement.

4. Update on the EC funded projects

4.1. 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 and to run six training workshops (in spring and autumn each year). Karel Vietsch gave some details about the trainees from the first four workshops. The fourth workshop was held on 25-26 May 2004 near Hamburg and was attended by 15 people from 10 countries.

He told the group that every TRANSITS training course could accommodate 20 people. The first three workshops were slightly oversubscribed, but there were only 15 participants in the last workshop in Hamburg. He was concerned whether the market has been exhausted and asked the group what should be done to attract more participants. Two more workshops would be organised which would mean 40 places. Karel Vietsch asked people to raise their hands if they expect one or more members of their CSIRT to attend to TRANSITS workshop during the next year. Altogether 23 participants responded.

Damir Rajnovic said that Cisco had their own vendor oriented CSIRT training with more emphasis on the products. He proposed to organise another workshop focused on the product vulnerabilities. It could be done by Cisco and some other vendor.

ACTION 12-01: Damir Rajnovic – to investigate the possibility to organise a workshop about product vulnerabilities.

Christoph Graf suggested to lower the requirements for participation in TRANSITS training courses and to make the website more attractive. He also thought that the TRANSITS courses should be advertised in a more timely manner.

Damir Rajnovic asked whether there were any follow-up with those people who have finished the TRANSITS courses already. It would be good to know whether they were working in the CSIRT area and have created new teams. Karel Vietsch replied that the TRANSITS project would distribute a questionnaire to all people who have participated in the TRANSITS courses.

A few other suggestions on how to market the TRANSITS courses were given.

ACTION 12-02: Wilfried Wöber – to investigate the possibility to announce the TRANSITS courses in the mailing lists of RIPE-NCC.

ACTION 12-03: Karel Vietsch – to create a short slide show for marketing the TRANSITS courses outside the NREN community.

4.2. Relation to GN2

Cristoph Graf spoke about GN2 relationship with TF-CSIRT. He gave an overview of the GN2 project including the project partners, data, structure, timelines, budget, and manpower. The project would start on 1 September 2004. The project has been specified for the first 18 months and TF-CSIRT would be interested in the details about Joint Research Activity 2 (JRA2). He mentioned all the JRA2 work items (WI) and paid special attention to those who were related to TF-CSIRT, i.e. WI4, WI5.

WI4 was the relationship with TF-CSIRT. The motivation for this relationship would be that the broader view of TF-CSITR could be useful for GN2/JRA2. The work item would imply creation of communication channels between the staff of NRENs working on JRA2 and TF-CSIRT, JRA2 progress report presentation to TF-CSIRT, forming the ad-hoc groups of TF-CSIRT experts for specific advice to JRA2, side-by-side or joint JRA2/TF-CSIRT meetings. Cristoph Graf mentioned two formal deliverables and who would work on these tasks (SWITCH and SURFnet).

He explained in detail the expected way of collaboration. He proposed that all NREN staff members working on JRA2 would join the TF-CSIRT mailing list. Separate JRA2 mailing lists should be used for non-disclosure things and to avoid overload on the TF-CSIRT list. For the ad-hoc groups JRA2 would look for volunteers, but there would be no obligations for TF-CSIRT to find them. Cristoph Graf thought that side-by-side meetings of TF-CSIRT and of the NREN staff working on JRA2 should be organised. He also asked TF-CSIRT to mention the collaboration with GN2 in the new ToR including the ad-hoc groups of experts and acknowledging the areas of common interest.

WI5 was the establishment of the advisory panel. Cristoph Graf explained the tasks of the panel. It should comment on the work carried out by JRA2, overview trends and evolution of the network security and incident handling, devise recommendations for work in the subsequent years of JRA2. The advisory panel would be recruited from TF-CSIRT and would consist of about 10 people. The panel meetings should be adjacent to the TF-CSIRT meetings. Cristoph Graf mentioned the deliverables and possible contributors for this work item as well. From TF-CSIRT he hoped to receive help in finding the panel members. The panel would be established in months 1-3 of the project, TF-CSIRT should discuss the panel in details in the next meeting in Malta. Cristoph Graf said that there were no resources available for the advisory panel and that it should be done on a self-funding basis.

Gorazd Bozic and Karel Vietsch pointed out that much communication about the JRA2 activities would be very detailed and only of interest to the relevant staff members of the twelve NRENs working on JRA2. Cristoph Graf agreed that for such things an internal list should be used, but the TF-CSIRT mailing list would be used to inform the whole community.

ACTION 12-04: Cristoph Graf – to prepare the draft document about the advisory board and to lead the discussion about it in the next TF-CSIRT meeting.

5. Update on Abuse forum meeting

Peter Quick presented information about the Abuse forum meeting which was held on Wednesday before the TF-CSIRT seminar. It was the 3rd meeting; there were 35 participants from 24 different ISPs and 10 different countries. That was much wider coverage than it was in Madrid.

There were three major working groups formed in the forum, they would focus on virus/worms, SPAM and copyright issues. The working groups could change in the future based on the actual problems. In future they would organise Abuse workshops twice a year to get in contact with other abuse teams. A name should be established for the forum; so far it was called "European Abuse Forum". A webpage and mailinglists should be set up to exchange information and to communicate directly with the forum. They planned to build a kind of "trusted network" for abuse teams, to make information exchange easier.

He summarised that Abuse forum meeting was very well attended; only 5 teams were represented for the second time. The considerable percentage of new teams did not allow making prognosis for the future. Peter Quick thanked for the possibility to report to the TF-CSIRT meeting.

Andrew Cormack proposed to present the Abuse forum in the national events, when the forum is established.

Gorazd Bozic asked if there were special requirements to join the forum. Peter Quick replied that so far there were no requirements; all major ISPs dealing with the abuse issues could join. In future the requirements should be devised. As examples of requirements he named possession of the AS number, number of customers, etc.

Gorazd Bozic asked whether they agreed to include Abuse forum in the Terms of Reference (ToR) of TF-CSIRT. Peter Quick replied positively.

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

Gorazd Bozic reported about the latest developments regarding the ENISA. He reminded the meeting that the ENISA function would be about advice and awareness-raising,and not regulatory. TF-CSIRT people have participated in the ENISA discussions and many of their comments have been addressed. ENISA was created on 1 January 2004; the seat of the agency would be in Heraklion, Crete, Greece. Gorazd Bozic was in the management board of the agency, as a representative appointed by the Slovenian government. The management board would meet in July 2004 and then they should appoint the director of the agency.

Karel Vietsch spoke about the tradition to have meetings between EC officials and TF-CSIRT representatives. Unfortunately Mr. Santucci, who was very enthusiastic, has been moved to another unit and TF-CSIRT representatives should establish contact with the new head of the unit – Mr. Jacques Bus. Karel Vietsch proposed to contact him and to organise the next meeting in September 2004. He asked whether there would be any volunteers from the group. Some people volunteered. The date of the meeting would be suggested by the EC; Karel Vietsch would inform the group.

ACTION 12-05: Karel Vietsch – to organise the meeting with the EC officials in September 2004.

Karel Vietsch said that the EC was very enthusiastic to have new security related projects and they would like to encourage the community to submit proposals for the next call. The next call would be in November 2004 with the deadline in January 2005. Karel Vietsch asked people to think about the possible projects, search for ideas, and discuss them in the mailing list. He also proposed to have a serious brainstorming meeting about the project proposals in Malta.

ACTION 12-06: Karel Vietsch – to initiate a discussion in the mailing list about possible new EC project proposals and to discuss them in the next TF-CSIRT meeting in Malta.

7. Improvements to CHIHT

Marco Thorbrügge spoke about the recent improvements of the clearing house service. He had sent a report to the mailing list as well. Moving basic tools into an own category and the re-organisation have been done. Adding more information to the CHIHT, particularly completing the information for the existing tools, was ongoing.

Marco Thorbrügge gave an overview on which information was available before the re-organisation and which had been added later. He illustrated his presentation with the examples from the webpage. As one of the problems Marco Thorbrügge mentioned giving the support for tools. As CHIHT was open to everyone it would be very easy to abuse the supporter. The solution could be to mention which teams used the particular tool and then people could find their details via the TI page and to ask for help.

The next phases of the re-organisation should be the creation of a new questionnaire, including working on the existing survey to gather new tools, and adding workflow descriptions. Marco Thorbrügge asked for volunteers to help him to gather the information. 7 people volunteered and Marco Thorbrügge summarised that it should be enough to complete the task. He hoped to have the next questionnaire and new tools by the next TF-CSIRT meeting.

He also asked people to send him information about the work flow of their teams. Some people volunteered to do that. Marco Thorbrügge agreed to encourage people in the mailing list to provide him with the information about the work flows.

ACTION 12-07: Marco Thorbrügge – to ask people in the mailing list to send him information about the teams' work flows.

Jan Heijblom asked whether there was a plan to synchronize the CHIHT with other data sources. Marco Thorbrügge replied that it was a good point and maybe that could be implemented in the future.

Gorazd Bozic asked whether the name of CHIHT would be changed. Marco Thorbrügge replied no, because the existing name CHIHT was quite wide known.

8. Update on IRT object issues and WG

Wilfried Wöber reported about the recent developments regarding the IRT object and working group (WG). Deployment had speeded up and some teams have tagged all the address objects of their constituency. He showed some statistics.

There has been another round of the discussions during the RIPE48 meeting. People were concerned that the IRT object would be too complicated to understand and use it. It has been proposed to make the attributes "signature" and "encryption" optional. Wilfried Wöber asked whether the group would agree to make these attributes optional. No one objected, so the RIPE-NCC could go on with the implementation.

Regarding the next steps Wilfried Wöber mentioned the idea to use other security technologies or resources, e.g. X.509 certificates, AS numbers. Some people expressed their support to use X.509 certificates. Ulrich Kiermayr thought that it would be possible to use X.509 already. Wilfried Wöber and Jan Meijer would investigate which certificates would be possible to use and how to extend this list.

ACTION 12-08: Wilfried Wöber and Jan Meijer – to investigate which certificates are possible to use for the IRT objects and how to extend this list.

Wilfried Wöber asked the opinion of the group regarding the additional "accreditation" plans for the IRT objects. Currently the "accreditation" could be done by TI or RIPE. Jan Meijer said that there were about 50 CSIRT teams "under" the SURFnet team and he would prefer to be able to approve their IRT objects. Wilfried Wöber summarised that it would be similar approach like with the "sub-CSIRTs".

Gilles André asked what the requirements to have an IRT object are. Wilfried Wöber replied that it was necessary to prove that the organisation has some constituency and it could be done with RIPE-NCC, without contacting TI.

Andy Bone asked whether it could be possible to have 2 or 3 CSIRTs associated with the same IP address block. Wilfried Wöber said that it is possible, but they all would have the same priority. Only with the comments it could be possible to prioritise one of them.

Wilfried Wöber informed the group that there would be only two RIPE meetings in the year 2005 and that he would give a presentation together with Don Stikvoort in the FIRST conference in Budapest about the IRT objects and relation among DB objects.

9. EISPP – Follow-up activities

Bernd Grobauer reported about the EISPP project follow-up. He said that it would be the last presentation in the TF-CSIRT meeting on the subject. The project has successfully ended, as was acknowledged by the EC in February 2004. He gave an overview of the project, its partners and objectives.

The final report of the project is available in the website, the Common Advisory Format and CEISNE Model and Processes have been developed and are available as well.

Bernd Grobauer gave an overview of the Common Advisory Format, explained its pros and cons, and showed an example. Regarding the future he hoped that the format would be used widely. So far the

format has been used among the project partners and some CSIRTs in Germany. There were some plans for co-operation between Latin-American CSIRTs and esCERT on basis of the EISPP format.

The overview of the related work was presented and the roadmap towards CEISNE was discussed. Bernd Grobauer hoped that the TF-CSIRT community would adopt the EISPP format, the new VEDEF working group would capitalize on their experience and could work on that. Bernd Grobauer would be happy to participate.

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

Ian Bryant gave an overview of the latest activities of the VEDEF WG. He started his presentation with an 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. He introduced the possible WG outputs and plan of activities.

Since the last TF-CSIRT meeting in Madrid the charter of the WG has been published and external activities have been reviewed. Regarding the collaboration with IETF one possibility could be to re-charter the INCH WG to include the VEDEF activity there rather than to create a new WG. He explained how the VEDEF WG could collaborate with the follow-up of the EISPP project and the relationship with CAIF.

Regarding the future Ian Bryant said that the EISPP format would be selected as the underlying vulnerability format. He informed the group that during the FIRST conference in Budapest there would be the INCH WG meeting, CAIF presentation and BoF on VEDEF. Ian Bryant encouraged people to participate in these events. He would like to activate the WG to draft the first document about the WG requirements. This document should be finalised during the next TF-CSIRT meeting in September 2004.

Regarding the working pattern he explained that a dedicated mailing list would be used and it would be run by TERENA. The WG would meet on the seminar day of the each TF-CSIRT meeting and during the FIRST conference.

Ian Bryant asked for volunteers who would like to contribute to this working group. Some people volunteered and Ian Bryant agreed to send a reminder to the TF-CSIRT mailing list.

ACTION 12-09: Ian Bryant – to send an invitation to the TF-CSIRT list to participate in the activities of the VEDEF WG.

11. Update on FIRST

Udo Schweigert reported about the latest activities in FIRST. The next FIRST conference would be held in Budapest Hungary, 13 - 18 June 2004. He gave an overview on the programme of the conference and encouraged people to attend the conference. For those who were not able to attend he reminded to take care of their proxies for the Annual General Meeting. The following FIRST conference would be held in Singapore in close cooperation with APCERT TF.

He presented the new FIRST membership process and compared it with the TI accreditation process. For getting the FIRST accreditation the site visit would be mandatory, 2 sponsors would be needed and the minimum size of team would be 2 people. This led to extensive discussions. People did not understand the need for the site visit and justification of the other requirements. Udo Schweigert clarified their concerns and explained the migration process. The main idea behind these changes was to increase the level of trust, although it would mean to loose teams with only 1 member. Regarding the site visit Udo Schweigert said that the Steering Committee can decide to make an exception. The discussion moved on to the notion of trust and data security issues.

12. IODEF: evaluated

Jan Meijer reported about the situation with the IODEF format. He reminded the goal of IODEF and the historical development. He summarised that the current usage of the IODEF format was very limited, only few CSIRTs were using it and it was not supported in the RTIR.

Jan Meijer explained the existing problems with IODEF, i.e. data model complexity, problems with the implementation, lack of protocol for the workflow, etc. He thought that if the protocol had not been needed for 5 years, maybe it would not be needed in the future as well. Some problem spaces would still remain, i.e. incident handling data, statistics gathering.

Regarding the future Jan Meijer proposed two possibilities. One would be to continue on the current path with contributing to INCH, continuing to work on the implementation of IODEF, and getting IHS implementators and users to adapt their systems and working methods to IODEF. The second option would be to focus on the incident-handling data exchange only within TF-CSIRT (TI) and not trying to solve the problems of the wider world. BIEN WG then could work on this goal and deploy blocks for an Incident-data Exchange Network.

Jan Meijer asked which solution would be preferred by the group. Andrew Cormack agreed that it would be wise to focus on the TF-CSIRT needs only, he supported the 2nd solution. Karel Vietsch expressed his surprise about the outcome of this presentation. Gorazd Bozic agreed that the WG should focus on building small pieces which are needed for them. No other comments were received.

13. Update on RTIR working group

Andy Bone gave an overview on the RTIR tool and the working group activities. The RTIR was the only open source incident handling tool. It has been widely used, including teams in Japan and the US. He presented the RTIR functionality and structure, including incident response, investigation, blocks, and incidents. Andy Bone emphasized the close cooperation with Best Practical Solutions LLC who was helping to customize the software.

During the last TF-CSIRT meeting in Madrid it has been decided to create a working group for the development of the RTIR software. The goal of the WG was to move to the 2nd version of the software which would be better adopted for the CSIRT requirements. 22 teams were interested in this software, 17 participated in the first WG meeting in Madrid. Later 5 teams came together in London and 8 teams participated in the video conference. Andy Bone announced a short WG meeting after this TF-CSIRT meeting as well.

The 1st version of the RTIR software was more JANET oriented, the 2nd version should be more advanced and more suitable for others. Andy Bone mentioned special areas of interest for the 2nd version and their status, including usage of GPG/PGP, XML formatting, multiple constituencies, information storage, templates, improvement of the look-up facilities, access to RT queues, reporting.

Andy Bone also noted that they were working on the code of conduct which would be based on the eCSIRT.net model. The communication would be carried on the TF-CSIRT mailing list, but they could create a separate mailing list if there would be too much traffic. Best Practical has released the documentation and Andy Bone could send the hard copies by post to those who were interested. The contract with Best Practical should be signed and TERENA would assist the working group in this matter. The support system and levels, i.e. bronze, silver, gold, were explained.

Jacques Schuurman said that SURFnet was encouraging the associated teams to use the RTIR. They experienced problems with the internal incident response, because it should be IP address based not email based. He asked whether anyone in the community had experience with this. Ulrich Kiermayr said that they have worked with this problem and offered to explain it off-line. Andy Bone added that it would be great if somebody could make this module.

Karel Vietsch asked whether the RTIT WG could transform into an EC project. Andy Bone said that the idea was nice, but they hoped to finish the 2nd version of the software before the end of year 2004, which would be too early for any project proposal.

14. The new ToR for TF-CSIRT

Gorazd Bozic explained the group that the existing Terms of Reference (ToR) of TF-CSIRT expired in May 2004 and if the group wanted to continue their activities, the new ToR should be devised and approved. The group expressed its support to continue the TF-CSIRT task force.

The draft of the new ToR has been prepared and was discussed by the group. The result of this discussion was the new ToR which would be presented to the TTC in September 2004. It can be found on line: http://www.terena.nl/tech/task-forces/tf-csirt/TSec_04_084-rev2.pdf

Points 1 to 9 of the ToR were accepted without changes, the group devoted more time to discuss the work items and the deliverables.

The work items A, B, D, E, H, K, and O (according to the previous list) were accepted without any discussions or changes.

Regarding the work item C "Incident Description and Registration Framework" Jan Meijer proposed to drop it. Although he had some concerns that, since IODEF was accepted in the Asia Pacific region, it could return to the area of interest for TF-CSIRT too. Karel Vietsch and Ulrich Kiermayr proposed some changes to the text. Jan Meijer said that he would not go to the IETF meetings anymore, but could report about the activities from the information in their mailing lists. Klaus-Peter Kossakowski thought that this work item should be kept in a shorter form. There would be the INCH meeting in FIRST and he hoped that there would be some people in the future who could report the group about the latest developments. The group agreed to the new formulation of the work item.

About the work item F "Training of new (staff of) CSIRTs" Wilfried Wöber asked clarification about the text. Karel Vietsch and Andrew Cormack explained their liabilities. The text was accepted without changes.

Przemyslaw Jaroszewski explained the text of the work item G "Assistance to the establishment of new CSIRTs" and asked the opinion of the group. He said that they would like to create a single point of contact for those who need help in establishing a new CSIRT. A webpage, different from the CERT.CC webpage would be useful as well. It should be more focused on easy accessible information like PP presentations not long documents. Gorazd Bozic said that the group should decide whether to keep this deliverable. Damir Rajnovic thought that another team which would do similar things like TRANSITS and CHIHT would not be needed. Karel Vietsch argued that there were not enough CSIRTs in Europe and TRANSITS had a very limited scope. People should have heard about CSIRTs before coming to TRANSITS. So the focus of this work item should be the awareness raising. Andrew Cormack explained his vision about this work item. The group discussed whether it should be the task of TF-CSIRT to raise the awareness and to promote the creating of the new teams. Gorazd Bozic said that, if some people formed the group, saw this problem and wanted to contribute to it, it would not mean that everyone should participate. Therefore he did not see anything wrong having it as a work item. Karel Vietsch proposed that maybe this work item could be transformed into the EC project with available funds for the site visits. Andrew Cormack told the group about his plans to meet the head of the CERT.CC team during the FIRST conference. Finally the group agreed to keep this work item.

Regarding the work item I "Emergency Backup Infrastructure" Karel Vietsch said that it has been discussed for last time in January 2003. If there would be volunteers who would like to work on this item then it should be kept, but otherwise he proposed to drop it. Gilles André said that he would be interested to work on it and asked for other volunteers. Jan Meijer thought that the 2nd part of the work item was already covered by the TI extra services. Klaus-Peter Kossakowski partly agreed but said that there would be space for some research as well. Gorazd Bozic asked for the other volunteers. No one else volunteered. The group voted whether to leave or to drop this work item. It was decided to drop the work item "Emergency Backup Infrastructure".

Marco Thorbrügge asked to explain what "BestPractical" meant in the work item J "Request Tracker for Incident Response". The group discussed which would be the best way to mention it and agreed to include the full name of the company – "Best Practical Solutions LLS". No other changes to the work item were made.

Regarding the work item L "Collaboration with the Joint Research Activity "Security" in the GN2 project" Jacques Schuurman asked whether the text about the advisory panel should be included. Christoph Graf said that it was included and approved in the JRA2 text and therefore should be in the TF-CSIRT ToR as well. Some grammatical changes were proposed and the text of the work item was accepted.

Andrew Cormack and Klaus-Peter Kossakowski thought that the work item M "Building Blocks for IODEF Exchange Network" should be dropped. Damir Rajnovic disagreed saying that some activities have been carried on and the work item should be kept. Jan Meijer proposed to keep the work item and to change "IODEF" to "Incident Data" in the title and some other changes in the text of the work item. After some discussions it was decided to keep the work item.

Klaus-Peter Kossakowski proposed to drop the work item N "eCSIRT.net Follow Up", because it was covered elsewhere. The group agreed.

Regarding the work item P "Liaison with the European Forum of Abuse Teams" Peter Quick expressed his concerns that the forum could change the name. He also proposed to include more activities in the ToR. Gorazd Bozic assured him that change of name would not be a problem, but other activities should be explained elsewhere. The work item was accepted.

After all the work items were discussed Gorazd Bozic asked to group to accept the new ToR. It was accepted unanimously. Gorazd Bozic said that if the new activities arose the group was eligible to modify the ToR.

15. 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.
Andrew Cormack said that a half day seminar in the future would give a time slot for the other activities for non-accredited teams. Gorazd Bozic agreed that the time slot should be used. No other comments were received.

16. Date of the next meetings

The next meeting will be held on 23-24 September 2004 in Malta (hosted by mtCERT). Martin Camilleri presented the venue of the next meeting and introduced the participants with Malta. He emphasized that the electricity plugs in Malta are the same as in the UK.

The subsequent TF-CSIRT meeting will be hosted by JANET-CERT in London, UK on 27-28 January 2005. The dates still could change.

Gorazd Bozic informed the participants that he has received offers to host a TF-CSIRT meeting from POL34-CERT, CERT.PT and SWITCH-CERT.

17. Any Other Business

The group expressed its thanks to DFN-CERT for organising a very nice meeting.

List of meeting participants

	Name	*Organisation*	*Country*
1.	Gilles André	CERTA	France
2.	Andy Bone	JANET-CERT	United Kingdom
3.	Peter Bovekamp	CERTCOM	Germany
4.	Gorazd Bozic (Chair)	SI-CERT	Slovenia
5.	Ian Bryant	NISCC R&D	United Kingdom
6.	Andreas Bunten	DFN-CERT	Germany
7.	Martin Camilleri	mtCERT	Malta
8.	Garaidh Cochrane	JANET-CERT	United Kingdom
9.	Andrew Cormack	UKERNA	United Kingdom
10.	Warren Daly	HEAnet	Ireland
11.	Aleksandor Diveski	MARNet	Macedonia
12.	Ralf Dörrie	Telekom-CERT	Germany
13.	Gary Dooley	Royal Mail Group	United Kingdom
14.	Jan Droemer	Philips	the Netherlands

15.	Serge Droz	SWITCH-CERT	Switzerland
16.	Michel Dupuy	CERTA	France
17.	Elaine Farmer	BTCERT	United Kingdom
18.	Lionel Ferette	BELNET	Belgium
19.	Mikhail Ganev	RU-CERT	Russia
20.	Natasa Glavor	CARNet	Croatia
21.	Christoph Graf	SWITCH-CERT	Switzerland
22.	Jon Grew	BT SBS	United Kingdom
23.	Bernd Grobauer	Siemens-CERT	Germany
24.	Peter Haag	SWITCH-CERT	Switzerland
25.	Jan Heijblom	KPN NL Fixed Net	the Netherlands
26.	Ian Hurst	NISCC	United Kingdom
27.	Przemyslaw Jaroszewski	CERT Polska / NASK	Poland
28.	Hans-Peter Jedlicka	CERT-Bund	Germany
29.	Richard Jones	BT SBS	United Kingdom
30.	Pavel Kacha	CESNET z.s.p.o.	Czech Republic
31.	Baiba Kaskina (Secretary)	TERENA	-
32.	Ulrich Kiermayr	ACOnet-IRT	Austria
33.	Piotr Kijewski	CERT Polska	Poland
34.	Frank Klein	Siemens-CERT	Germany
35.	Jan Klever	DFN-CERT	Germany
36.	Jan Kohlrausch	DFN-CERT	Germany
37.	Klaus-Peter Kossakowski	DFN-CERT	Germany
38.	Andrea Kropacova	CESNET z.s.p.o.	Czech Republic
39.	Arttu Lehmuskallio	TeliaSonera Finland Abuse	Finland
40.	Antonio Liu	PRESECURE	Germany
41.	Miroslaw Maj	CERT Polska	Poland
42.	Chelo Malagón	IRIS-CERT, RedIRIS	Spain
43.	Mally Mclane	JANET-CERT	United Kingdom
44.	Stelios Maistros	GRNET-CERT	Greece
45.	Jan Meijer	SURFnet / CERT-NL	The Netherlands
46.	Tassos Moschos	GRNET-CERT	Greece
47.	Tom Mullen	BTCERTCC	United Kingdom
48.	Sergey Linde	RU-CERT	Russia
49.	Gustavo Neves	FCCN (CERT.PT)	Portugal
50.	Tomasz Nowocien	POL34-CERT	Poland
51.	Matthias Oberlinner	Siemens-CERT	Germany
52.	Mark Pattinson	NISCC	United Kingdom
53.	Peter Quick	Telekom-CERT / T-Com	Germany
54.	Damir Rajnovic	Cisco Systems	United Kingdom
55.	Maria Rådström	Telia Abuse	Sweden
56.	Juergen Sander	PRESECURE Consulting GmbH	Germany
57.	Lino Santos	CERT.PT	Portugal
58.	Jacques Schuurman	SURFnet / CERT-NL	The Netherlands
59.	Udo Schweigert	Siemens CERT	Germany
60.	Mikel Stamm	DK-CERT	Denmark
61.	Harri Sylvander	Funet CERT	Finland
62.	Marco Thorbrügge	DFN-CERT	Germany
63.	Christopher Trauner	Siemens-CERT	Germany
64.	Maris Urkis	LITNET CERT	Lithuania
65.	Karel Vietsch	TERENA	-
66.	Wilfried Wöber	ACOnet-IRT	Austria
67.	Michal Zakrzewski	Versatel Telecom	the Netherlands
68.	Jörg Zemke	Philips	The Netherlands

Apologies were received from:

Roberto Cecchini	GARR-CERT	Italy
Per Arne Enstad	UNINETT CERT	Norway

Carles Fragoso	CESCA-ERIAC	Spain
Oliver Goebel	RUS-CERT	Germany
Kauto Huopio	FICORA / CERT-FI	Finland
David Parker	UNIRAS/NISCC	United Kingdom

RESULTING ACTION ITEMS

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	Christoph Graf	Circulate GN2 JRA2 related relevant documents to the TF-CSIRT mailing list.
12-01	Damir Rajnovic	Investigate the possibility to organise a workshop about product vulnerabilities.
12-02	Wilfried Wöber	Investigate the possibility to announce the TRANSITS courses in the mailing lists of RIPE-NCC.
12-03	Karel Vietsch	Create a short slide show for marketing the TRANSITS courses outside the NREN community.
12-04	Cristoph Graf	Prepare the draft document about the advisory board and to lead the discussion about it in the next TF-CSIRT meeting.
12-05	Karel Vietsch	Organise the meeting with the EC officials in September 2004.
12-06	Karel Vietsch	Initiate a discussion in the mailing list about possible new EC project proposals and to discuss them in the next TF-CSIRT meeting in Malta.
12-07	Marco Thorbrügge	Ask people in the mailing list to send him information about the teams' work flows.
12-08	Wilfried Wöber, Jan Meijer	Investigate which certificates are possible to use for the IRT objects and how to extend this list.
12-09	Ian Bryant	Send an invitation to the TF-CSIRT list to participate in the activities of the VEDEF WG.