Proposal for restructuring TF-CSIRT and the Trusted Introducer Service

Executive Summary

A proposal to better integrate TF-CSIRT and Trusted Introducer under the TERENA structure. The goal is to streamline operation without any radical change, whilst establishing a unified regional group with a recognisable membership. Another aim is to improve coordination and use of staff resources, as well as establish a more direct relationship between CSIRTs and the TF-CSIRT leadership.

1. Introduction

The Task Force for Computer Security Incident Response Teams (TF-CSIRT) operates under the auspices of the Trans-European Research and Education Networking Association (TERENA). It was originally established in 2000, and since then has established itself as one of the main forums where CSIRTs from a variety of sectors can come to discuss and exchange experiences and knowledge. Indeed, TF-CSIRT is not only TERENA’s longest running task force, but is by far the most successful in terms of participation.

The average attendance at TF-CSIRT meetings is between 60 and 70 participants, although this rises to approximately 120 participants for the annual meetings held jointly with FIRST. In the past year, around 60% of participants have come from academic CSIRTs, 20% from government CSIRTs, 15% from commercial CSIRTs, and 5% from other types of organisations.

Over the years, TF-CSIRT has worked on a number of activities useful to CSIRTs and network security professionals, as well as providing advice to organisations such as the European Commission, ENISA and national governments. It has also established liaisons with other global and regional CSIRT organisations including FIRST, APCERT and OIC-CERT, and has collaborated in the various GÉANT projects. In addition, TF-CSIRT has established a number of spin-off activities that include the Trusted Introducer (TI) service, the popular TRANSITS Training Courses, and upgrading the RTIR software that is actively used by many CSIRTs.

A particularly important activity is Trusted Introducer that was established in 2001 as an accreditation and listing service. This is financed by the accredited CSIRTs and provided under contract by a third-party company (originally S-CURE, but PRESECURE since 1 September 2011). There are currently 80 accredited teams of whom 44% are academic, 28% are governmental, and 28% are commercial; as well as 143 listed teams of whom 39% are academic, 24% are governmental, and 37% are commercial. The average attendance at each meeting of TI-accredited CSIRTs is around 50 participants.

It is therefore clear that TF-CSIRT has moved well beyond its origins as a forum for academic CSIRTs, and is increasingly seen as a representative body by external organisations. However, in common with all TERENA task forces, the
group’s mandate and terms of reference still need to be renewed by the TERENA Technical Committee (TTC) every two years. This has become incongruous for a group that is now indispensible, but which deals as much with political and administrative issues as technical activities.

Furthermore, TF-CSIRT has no formal notion of membership which is increasingly expected by external organisations, and there is a confusing overlap between TF-CSIRT and TI. Although the participation in both is very similar, they often have different Chairs and Secretaries which leads to duplication of function and at times awkward coordination. The current division of labour between TERENA and the TI contractor also does not permit common use of staff resources, which can be problematic where a particular task falls into a different area of responsibility. For example, the TI Review Board often identifies tasks that would be better handled within the context of TF-CSIRT, but there is no clear way of enabling this.

More importantly though, there is a concern that TF-CSIRT is drifting away from its former cooperative approach as there is increasingly less input from the participants. The Chairs and Secretaries have to spend more time putting together programmes, which in turn accentuates the impression that participants can have little input into the direction of the group. Whilst this is somewhat inevitable as a group grows to the size of TF-CSIRT, the fact there are few candidates standing for the TI Board positions also suggests the CSIRT community has become a bit disconnected from the leadership. This is even more of a concern now that non-academic CSIRTs constitute a (paying) majority, as they are not represented through other TERENA bodies (such as the General Assembly and Executive Committee) and therefore have little influence on appointees.

It is therefore proposed to formally incorporate TI within TF-CSIRT, whilst establishing a formal membership for TF-CSIRT based on the accredited, listed and associate categories of TI. Whilst this would not represent a significant departure from current arrangements, it is envisaged that it would create a more streamlined, coherent and efficient structure than at present. This is important if TF-CSIRT is to maintain and extend its stature as the pre-eminent CSIRT forum in the European region, and of course encourage CSIRTs to subscribe to its services.

An outline of the proposed changes was presented during the TF-CSIRT meeting on 2 June 2011 and nearly all of the 63 participants were favour, with no objections. At the request of the group, more detailed proposals were circulated for comment to a working group comprised of Serge Droz (SWITCH CERT), Lionel Ferette (TF-CSIRT Chair), Przemek Jaroszewski (CERT Polska), Baiba Kaskina (CERT.LV), Jacques Schuurman (XS4ALL), Erika Stockinger (CERT-SE), Toomas Lepik (CERT-EE) and Wilfried Woebber (ACOnet CERT), and their feedback has been incorporated into this document.

2. Membership

There is currently no formal membership of TF-CSIRT and meetings and the mailing list are in principle open to anyone with a bona-fide interest in incident handling and network security. The approval of the Chair is technically required for individuals to attend meetings or subscribe to the mailing list, but whilst this procedure has not really been problematic to date, in practice it is somewhat ad-hoc and increasingly impractical.

As there is need for higher levels of assurance with respect to the discussion of certain sensitive information, Trusted Introducer does organise a half-day session
in conjunction with TF-CSIRT meetings that only accredited CSIRTs may attend. However, the holding of such meeting under a different name requires a separate registration process and sometimes causes confusion amongst attendees (particularly at the joint meetings with FIRST).

For various reasons, external organisations are also increasingly asking who the TF-CSIRT members are, which invariably leads to a convoluted explanation about the difficulty of defining a membership from a mailing list of individual subscribers. However, the TI service does have clearly defined categories for CSIRTs (namely 'Accredited' and 'Listed'), and whilst TF-CSIRT and TI are not entirely synonymous, the CSIRTs in these categories could be considered the basis of a ‘membership’.

It is therefore proposed that three membership levels are created, based on the existing TI categories. Admission to a particular level would be automatic upon accreditation or listing in accordance with the existing TI procedures. Similarly, membership would be downgraded upon de-accreditation, and lost upon de-listing by TI.

**Accredited Members** – Recognised CSIRTs that meet and maintain the defined standards for accreditation, and who continue to pay the necessary TI subscription fee. Registered employees of such members would have right of access to all TF-CSIRT meetings (including sessions for Accredited CSIRTs only) and all documentation. Accredited Members would also have voting rights.

**Listed Members** – Recognised CSIRTs that have successfully applied for this status in accordance with the requirements for TI ‘listing’. Registered employees of such members would have right of access to TF-CSIRT meetings except the sessions for Accredited CSIRTs only, as well as certain documentation. Listed Members would not have voting rights, although a TI subscription fee would not be charged.

**Individual Members** – Individuals working in incident response or network security who are not currently employed by an Accredited or Listed Member, and who meet and maintain the defined standards for TI Associate status. Such members would have right of access to all TF-CSIRT meetings (including sessions for Accredited CSIRTs only) and all documentation, but would not have voting rights. Individual memberships would have to be renewed on an annual basis, although a TI subscription fee would not be charged.

As TF-CSIRT does not wish to discourage potential new members, nor individuals who can provide useful input to the community, it is proposed that the TF-CSIRT Chair retains the possibility to invite non-members to meetings, on a meeting-to-meeting basis. Such individuals could also be invited to sessions of Accredited Members if there are no objections from those members.

The introduction of membership may mean that some individuals on the TF-CSIRT mailing list may technically become ineligible to be subscribed. It is therefore proposed to ‘grandfather’ any such individuals into the new system for a given period (e.g. one year), but encourage them or their CSIRT to apply for membership. The TI mailing lists should not require any changes beyond renaming, as they are already restricted to TI Accredited CSIRTs and TI Associates.

### 3. Administration

TF-CSIRT is directed and coordinated by the Chair (currently Lionel Ferette) who is appointed by TERENA. There is no defined term of office (provided the Task
Force mandate is renewed), so in practice the Chair holds the position indefinitely until they wish to relinquish it.

The Chair is assisted by the Secretary (currently Kevin Meynell) who is a TERENA staff member. He or she organises meetings, prepares the programme, produces the minutes and proceedings, handles communications with the TF-CSIRT community and external bodies, and is responsible for the TF-CSIRT website and mailing list. Since 2008, he or she is also responsible for managing the TI contract and represents TERENA on the TI Review Board.

The TI Review Board exists to review the performance of the TI service, to make suggestions and recommendations with respect to the service components, and to make decisions with respect to the listing, accreditation and certification of CSIRTs. It is in principle appointed by TERENA who have responsibility for the TI contract, but three of the members are nominated by the accredited CSIRTs on a three-year cycle through an election process. The other members are the TF-CSIRT Chair and a representative of TERENA who is usually the TF-CSIRT Secretary. The Review Board members elect a Chair from within their midst on an annual basis, which is necessary as the composition of the Board changes from year-to-year.

It is proposed to establish a single Chair who would be nominated by the Accredited Members through an election process. The term of office would be three years, with the incumbent required to stand down at the end of this term.

The aim is to eliminate the confusion of having separate Chair positions for TF-CSIRT and TI, whilst giving the TF-CSIRT participants the opportunity to select a leader. In particular, it is important to give non-academic CSIRTs this opportunity given that they now outnumber the academic CSIRTs and have no representation elsewhere in TERENA.

A one-term limit on the Chair position is suggested as chairing can require a significant amount of work and incumbents should not feel obligated to continue in this position as has been the case in the past. In addition, a regular change of occupant should ensure that new ideas continue to be brought forward.

It is also proposed to transition the existing TI Review Board into a TF-CSIRT Steering Committee with an enhanced role. This would include the Chair and Secretary, as well as three nominated representatives as now. The nominated representatives would serve three-year terms, with one representative elected per year. However, it is suggested to introduce a single term limit for these representatives instead of the current two-term limit, for similar reasons as for the Chair.

As well as assuming the functions of the TI Review Board, it is anticipated that the Steering Committee would provide input into meeting programmes and direction as to the activities that TF-CSIRT should be undertaking. This is important in order to ensure that TF-CSIRT continues to focus on the right matters, is in contact with all relevant parties, and that the quality of meetings remains high. Steering Committee members would also deputise for the Chair in his or her absence.

It should be noted that whilst the elections would be held for the Chair and Steering Committee members, they would officially be the nominations of the TF-CSIRT community and would need to be formally approved by TERENA. It is unlikely that approval would be withheld, but as TF-CSIRT is a body of TERENA, TERENA needs to ensure that its activities are in line with the general principles of the organisation.
4. Activities

The current work of TF-CSIRT can essentially be broken down into knowledge transfer, development, liaison and training categories, with specific activities being outlined every two years or so. There are also the TI service activities that are periodically defined by TERENA in consultation with the TI Review Board.

It is not within the scope of this document to make detailed proposals about which activities should be undertaken as a successful task force needs to be dynamic and able to quickly respond to developments as they happen. The goal is establish a streamlined and efficient structure that can better identify the requirements of the community, with staff effort made available to support these.

Nevertheless, it is proposed to bring the TRANSITS training courses back under the umbrella of TF-CSIRT. These evolved out of TF-CSIRT and were run in the context of an EU-funded project from 2002 until 2005, after which they continued as a TERENA-organised activity. Whilst the courses remain popular though, they rely heavily on TF-CSIRT participants for tutors and course material, and this process should be better coordinated if the TRANSITS I and TRANSITS II courses are to meet expectations in future. In particular, TF-CSIRT could be better utilised to identify potential tutors at national and regional levels.

It is expected that the existing TI services will continue to be provided as these have already been subject to a recent review process. Nevertheless, it is proposed that the TF-CSIRT activity programme (currently incorporated in the Terms of Reference) is reviewed and updated every year rather than every two years as at present. This will ensure staff resources can be more efficiently targeted at relevant and useful tasks.

5. Staff Support

TERENA provides administrative support to TF-CSIRT and manages the TI contract on behalf of the CSIRT community. This is work requires around 0.3 FTEs and is mostly undertaken by the appointed Secretary.

The TI services are provided by a third-party company (currently PRESECURE) according to an agreed specification and service level agreement. They are six named members of staff who work on these services as needed, although other members of staff can be called upon if specialist skills are required. Extra work undertaken outside of the scope of the contract is subject to an additional charge.

It is not envisaged these arrangements will change for the foreseeable future, although it is recommended that the TF-CSIRT Secretary has more oversight of the programme for the Accredited CSIRTs’ sessions during TF-CSIRT meetings. This would be in addition to the rest of the programme, with the aim of avoiding duplication which has occasionally happened in the past.

6. Website

The TF-CSIRT website (http://www.terena.org/) is hosted by TERENA, whilst the TI website (https://www.trusted-introducer.org/) is hosted by PRESECURE.

PRESECURE is contracted to renew the current TI website and this should be done in consultation with the TERENA Secretariat to ensure a “look and feel” that is in line with TERENA’s overall presentation. The TI team and the TF-CSIRT Secretary who are responsible for maintaining the websites, should also work
together to streamline the presentation of information and make appropriate cross-references etc..

7. Funding

The cost of providing administrative support to TF-CSIRT is currently in the order of EUR 24K per year. This includes secretarial support (including travel to meetings), and provision of the website and mailing lists.

TF-CSIRT is considered a support activity of the GN3 (GÉANT) project, so its costs are presently recouped from that project’s funding. Given that TF-CSIRT will continue to support the NREN community as well as maintain a service development aspect, it is anticipated that TERENA’s costs can continue to be recovered from the project until at least 31 March 2013.

The TI services are currently facilitated by an external company (PRESECURE from 1 September 2011 until 31 August 2014) under contract to TERENA. These services are provided on a unit price basis, with TERENA re-charging these costs to accredited CSIRTs. TERENA previously covered the costs of managing the contract from its own resources, but following a decision of the TERENA GA, will recoup these costs from the accreditation fees from 1 September 2011. Following a recent competitive tender exercise though, an improved contract was negotiated with the result that accreditation fees need not increase.

It is therefore proposed to largely maintain these financial arrangements, although some consideration needs to be given to the funding of TF-CSIRT when the GN3 project finishes.

The costs of staging meetings are currently covered by TF-CSIRT participants on a voluntary hosting basis. This has become an increasingly expensive undertaking for hosts given the rising numbers of participants and increased expectations of facilities at the venues. Nevertheless, there are sufficient volunteers to host the regular TF-CSIRT meetings (those usually held in May and September) for the next couple of years, and it should therefore not be necessary to charge registration fees for at least this period.

The joint meetings with FIRST (those usually held in January) need to be handled differently though, as they currently attract approximately 150 participants and have effectively become mini-conferences. Given the logistical requirements for such events, it is likely that some sort of registration fee will have to be charged in future unless substantial sponsorship can be found on a regular basis, or in the unlikely event that surpluses from accreditation fees rise to a sufficient level. However, registration fees should only be set at a cost recovery level.

8. Name

The name ‘TF-CSIRT’ is long-standing, descriptive and well known in the CSIRT community, whilst the name ‘Trusted Introducer’ is used to distinguish the accreditation and listing service. However, having two distinct names does not make it clear that TI is closely related to TF-CSIRT and causes some confusion outside and even within the European CSIRT community.

It is therefore proposed to rename Trusted Introducer to ‘TF-CSIRT Trusted Introducer’ to make it clearer that it’s a TERENA service under the auspices of TF-CSIRT. This should appear on all websites and documentation, along with appropriate references to TERENA.
The logos that CSIRTs display on their own websites need renewal, and this is closely related to updating of the websites mentioned in Section 6 above. The TI team should liaise with the TERENA Secretariat to ensure that the logos are in-line with TERENA’s overall presentation.

9. Expansion

Attendance at the TF-CSIRT/TI meetings every May and September have remained relatively static in the past few years, whilst those for the joint meetings with FIRST every January have consistently grown. Whilst it might be concluded that participants who don’t attend all TF-CSIRT meetings are specifically targeting this event, it might also be the case that there is more value in meeting with CSIRT personnel from different regions and sectors.

Similarly, whilst the number of CSIRTs that are accredited or listed with TI have consistently grown by about 3-5% per year, many of these never actively participate in TF-CSIRT or TI. More concerning though, some CSIRTs have started to withdraw from TI which is partly down to the current economic situation, but also because of the perception that TF-CSIRT and TI are primarily for academic CSIRTs and are therefore of limited value to CSIRTs in commercial and other sectors.

TF-CSIRT has recently started to liaise with the Grid and ccTLD community, but some effort should also be directed at better engaging CSIRTs in the law enforcement and defence sectors, as well as facilitating national liaisons where no initiatives currently exist. By bringing together CSIRTs from multiple sectors, it would add value for all participants whilst enhancing the status of TF-CSIRT as the main forum for CSIRTs within the European region.