

Request for Comments from the TF-CSIRT Community

On behalf of TF-CSIRT, the TI Review group is currently undertaking phase one of a two-part review to support the future service developments of Trusted Introducer. Phase one runs from May 2015 until December 2015 and is focusing on a review of current services provided by TI and future service needs. The TI Review group has met 3 times and would like to make the following recommendations to the TF-CSIRT community.

A. CHANGES TO TENDER REQUIREMENTS

1. **CA and X.509 Certificates:** the tender should not specifically ask for a CA but instead detail the need for a secure website with managed restricted areas and appropriate credentials for team members. This should be a complete solution and not require teams to purchase additional products (e.g. certificates, hardware tokens etc.). This should include requirements for credentials that can interoperate with the SAML event management services offered by GÉANT.
2. **Certification:** introduce a change to the certification process so that certifications are carried out by a small group of experts from the community (which could include TI staff) similar to the TRANSITS tutors model instead of only managed by TI staff.
3. **Communication Tools / Processes:** alerting services and IRC servers and not required by the community and should not be included in future service offerings.
4. **Communication Tools / Processes:** incident / vulnerability coordination should not be a requirement of the tender but could be offered on a best efforts basis.
5. **Communication Tools / Processes:** IRT object process is no longer required as RIPE does not make use of this and is changing its data gathering processes.
6. **Database API:** Introduce a requirement in future tenders for an API to the TI database.
7. **Maturity Testing:** subject to further testing, introduce a requirement in future tenders for regular maturity testing.

B. CHANGES TO ADDRESS IN CURRENT SERVICE PERIOD

1. **Listing / Accreditation:** ask the TI team to complete a short internal audit to ensure that all appropriate alerts around listing / accreditation are being delivered.
2. **Listing / Accreditation:** ask the TI team to flag listed teams that received listing status before the requirement for support was introduced and accredited teams that

may have received accreditation status without explicit support.

3. **Listing / Accreditation:** introduce a new process for listing whereby teams that do not update or actively confirm data is up-to-date within a three-year period automatically become unlisted.
4. **Meeting Support:** ask the TF-CSIRT SC and TI team to review the process for managing entry to the closed meeting and whether more effective approaches could be used.
5. **Meeting Support:** move management of the agenda for both closed and open meetings to the GÉANT secretariat to allow for more consistency in meeting management process and work with presenters to more accurately reflect TLP status. This could include moving out of closed session at different times when appropriate.

C. RECOMMENDATIONS THAT FALL OUTSIDE OF THE REVIEW PROCESS

1. **Accreditation Documentation and Support:** ask the TF-CSIRT SC to manage a review of the accreditation process documentation and proposed appropriate updates.
2. **Accreditation Documentation and Support:** work on the accreditation “package” to see how we are marketing it to the teams and review whether enough is offered in accreditation and provide more materials to help teams explain the value of accreditation to management.
3. **Listing Requirements:** consider using mature CERTS to help encourage other CERTS within their region to keep listing information up to date.
4. **Service strategy:** ask the TF-CSIRT to work on a strategy document for TF-CSIRT / TI and a mission statement for the service offering. This should include clarity on the goals of each of the current processes (listing, accreditation, certification). This will be further informed by phase 2 of the review process and should include the full current and future portfolio for TF-CSIRT (e.g. TRANSITS, training exercises etc.)

You are invited to respond with comments on these proposals via signed e-mail to: nicole.harris@geant.org or directly to the TF-CSIRT list. Comments on the proposals, additional changes to the service portfolio and proposals for future service requirements are welcomed. All responses should be sent by 5pm CET on 11th November 2015 at the latest.

Further information about the TI Review group and the Terms of Reference for the group can be found at: <https://www.terena.org/activities/tf-csirt/ti-review.html>. Full minutes of the meetings of the group are available on request.