Brussels, March 24, 2010

CENTR Comment in response to the consultation on the Domain Name System-Computer Emergency Response Team (DNS-CERT) Business Case

We have read with interest the business case for the DNS-CERT (http://www.icann.org/en/public-comment/#dns-cert).

All CENTR members are deeply involved in maintaining security and stability of the DNS, often beyond the scope of their own activity as top level domain managers. Therefore we fully support the renewed focus on Security in the ICANN strategic plan and share some of the goals of the DNS-CERT business case. However we would like to highlight some concerns in relation to this initiative.

First of all we believe it would be very helpful to identify those parties that have asked for this initiative as it would make clear what the exact needs are that they want it to fulfill. In response to a question asked at our last General Assembly, no CENTR Member indicated that it felt the need for a DNS-CERT as described in the Business Case. Members referred to existing initiatives and groups such as CERTs and FIRST and the trust networks that exist amongst internet infrastructure operators as the reason why they did not need a new organization. The CENTR community is very much prepared to bring on board those that are currently not as well connected as they should be.

The stability and security of the Internet is depending on much more resources than the DNS. The so called “Conficker issue” which was identified in the business case as a reason to start up a DNS-CERT was initially related to a security issue caused by a worm and was not a DNS problem. It is therefore a perfect illustration of the fact that security relies fundamentally on cooperation and collaboration amongst different experts and that’s how the current security network is build up. In such a framework different security incidents can be addressed more effective and on the long run much more efficient than with the proposed concept of a CERT focusing on one single area with potential security problem, like DNS. The key communication problem with Conficker was related to spontaneous unilateral communication through the ICANN channels in parallel to well established security networks. With agreed, tried and tested procedures the issues that occurred could have been prevented.

As raised by many at the ICANN meeting in Nairobi, we agree that this initiative overlaps with the work and goals of existing organizations such as the CERTs, OARC and FIRST. These organizations are also better positioned to assess the need for additional channels, given their expertise in this area. While the proposal states clearly that it explicitly wants to “avoid duplication of existing efforts and information sharing mechanisms” we feel a need for more information on

CENTR vzw/asbl
Belliardstraat 20
1040 Brussels – Belgium
tel +32 2 627 55 50
fax +32 2 627 55 59
secretariat@centr.org
http://www.centr.org

---

how that could be achieved. Many ccTLDs are already deeply involved in their local and national CERTs and they feel confident that the work by those CERTs is shared efficiently across the globe. Support for those ccTLDs without cooperation with their local CERTs can be arranged within existing organizations.

As was suggested during one of the Nairobi sessions, ICANN should focus first on sharing information about actions undertaken by these organizations, in order to build a common assessment of risks and weaknesses. This should also enable ICANN to clarify the exact scope of its initiative, since many questions were raised on that issue in Nairobi and during the CENTR Assembly in Warsaw. Only then would it be relevant to discuss whether new structures are necessary.

Our final concern relates to the funding of this plan. It is unclear on how this fits into the budget and operational planning. While the business case underlines that it should not be funded by ICANN, it also assumes that funding will be found after the start-up phase. CENTR feels that good business practice does not allow starting a project of such a scale and postponing discussions on funding until later. We therefore urge ICANN to ask the right question in the next phase of this consultation: ask an additional question to those who indicate DNS-CERT is needed to find out if they would be willing and able to pay for it.

In summary we recommend that these initiatives should not be rushed through. We believe it would be much better, cheaper, more efficient and quicker to support existing initiatives and find out from those that feel not well connected what prevents them from being in touch with the existing initiatives. The CENTR community is fully committed to enhancing the security and stability of the DNS and in particular we are prepared to support and help those ccTLDs in addressing those needs.

CENTR and its members therefore support to invest more work in assessing the current risks and weaknesses in close cooperation with all stakeholders including ICANN and we remain available to contribute to this discussion.

About CENTR

CENTR, the Council of European National Top Level Domain Registries, is the world's largest of Internet domain name registries. CENTR has over 50 members which account for over 85% of the country code domain name registrations worldwide. Each CENTR Full Member operates a country code top level domain. In this capacity they play a pivotal role in the stability of the Domain Name System and the Internet.

CENTR vzw/asbl
Belliardstraat 20
1040 Brussels – Belgium
tel +32 2 627 55 50
fax +32 2 627 55 59
secretariat@centr.org
http://www.centr.org