**INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY (ICTA)**
**The Celicourt 6, Sir Celicourt Antelme Street Port Louis Mauritius**
**Tel.: (230) 211 5333 Fax: (230) 211 9444 email: icta@intnet.mu**

# Procurement of Cloud-based Child Sexual Abuse (CSA) Filtering System at the ICT Authority, Mauritius.

Procurement Ref. No: **ICTA/OIB/CSA/04-20/04**

## Questions & Answers

**Q1:** CSA solution needs to be deployed on cloud network. Does ICTA have its cloud infrastructure or does bidder need to host on any public cloud network? Any preferred Cloud network from ICTA?
ICTA does not have its own cloud infrastructure. Bidder to provide same. No preferred cloud network.

**Q2:** The connectivity from each of the ISP & MSP (Mobile service provider) will be over dedicated IP network or secure public Internet. The Connectivity will be managed by service provider or ICTA. Please confirm the understanding.
It will need to be via secure public internet. Connectivity to be managed by service provider.

**Q3:** What is Bandwidth or number of requests per second which will be steered from each ISP/MSP towards CSA system.
In the present CSA filtering system, only BGP traffic (and not data traffic) is exchanged between ISPs and the CSA filtering service provider. It is only in the case of a blacklisted URL detected that it is redirected to CSA cloud filtering setup. The stats for same is available at https://www.icta.mu/stats_cyber.html

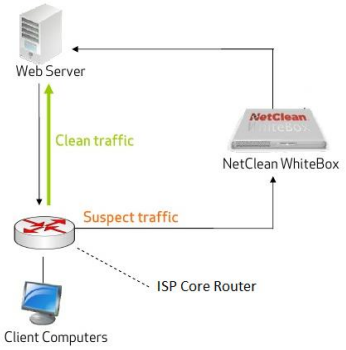
**Q4:** Does ICTA or ISP/MSP has IWF subscriptions?
No, the solution provider will need to do needful

**Q5:** How many Blacklist are required in solution. Only feed from IWF or local Blacklist from regulatory agency.
Only feed from IWF

**Q6:** In current solution, is the complete DNS traffic from each ISP/MSP routed to CSA system or only the uplink web traffic of blacklisted websites is routed to CSA system using BGP?
Only the uplink web traffic of blacklisted websites is routed to CSA system using BGP

**Q7:** If the solution is based on Uplink web traffic of blacklisted websites to CSA system based on BGP then traffic which not part of blacklist, will it exits to Internet from CSA system or it is routed back to ISP/MSP?
Clean traffic which is not blacklisted does not transit via the CSA system.

**Q8:** Please provide a diagram of the existing technical network architecture, and information on the CSA solution that has been implemented and in use at ICTA until 2020?




**Q9:** Will there be any need to integrate the CSA solution to any third party system(s)? If yes, please provide detailed information on the system(s)?
No

**Q10:** What is the total combined incoming / outgoing throughout for all telcos / ISPs? The Bid document says 42.5 Gbps inbound / 42.5 Gbps outbound, however, in recent discussions a total throughput of 10Gbps was mentioned. Is the 10Gbps mentioned the total throughput for Mauritius or the volume of traffic going over the VPN for the current CSA filtering solution?
Please stick to bid document information

**Q11:** What percentage of your TOTAL throughput will be BGP traffic directed to the filtering solution?
The only information is in terms of the actual traffic directed to the filtering solution as detailed out at
https://www.icta.mu/stats_cyber.html

**Q12:** It is assumed that a 3 year log retention period is required. If this is not required, how long must logs be retained? Are these logs expected to be stored on bidder's cloud storage or will ICTA provide their own storage / SAN?
3 year log retention period will be required to be stored on bidder's cloud storage

**Q13:** Are you able to provide us with more detail on the current solution as follows – average number of requests filtered per second? Average log file size?
See answer to question 2 above

**Q14:** With regard to the following requirement – *"(vii) The system should be able to filter down to the level of folders or even individual documents and images on a website. (E.g. you could filter http://www.website.com/badcontent but allow http://www.website.com/goodcontent)"* and *"(xi) – Bidders should explain if the proposed system can cater for Mauritian Internet user attempting to access HTTPS CSA websites based locally and internationally at the same level of granularity as described at para (vii)"* – the proposed system is only able to achieve this level of filtering on HTTP webpages, however, this is not possible for HTTPS webpages (where the entire top level domain is blocked – i.e. www.website.com) without SSL decryption. This is a common technical limitation for any solution on the market and our assumption is therefore that your current BGP solution is not able to deliver this for HTTPS websites. We do offer SSL decryption

however this would require ICTA to have the capability to install SSL certificates on all end user devices.
No SSL decryption required for now.

**Q15:** Further to the above and with reference to point (i), block pages can only be displayed on HTTP webpages, however, HTTPS webpages will still prevent access to CSA websites. In this case, a standard error message will be displayed (i.e. with the error message "your connection is not private"). Should the end user choose to "proceed anyway", they will then be served with an official / customizable ICTA / Government deny page.
Agreed

**Q16:** Please confirm whether ICTA is aware that in order to do per URL filtering (down to individual file / folder level), SSL Decryption is required with ICTA also having the ability to install SSL certificates on all end user devices in Mauritius?
Please see answer to question 5 above

**Q17:** With regard to the following requirement – *"(x) Bidders should explain if the proposed system can cater for Mauritian Internet users attempting to access CSA websites hosted locally and internationally via anonymous proxy servers without blocking other online contents accessed via anonymous proxy servers."* – it is certainly possible to block access to CSA websites that are accessed via anonymous proxy servers, however, we are unable to differentiate which content accessed via proxy websites is CSA content or other content. Anonymous proxies are by nature private and it is therefore not possible to allow good content accessed via proxy yet filter bad content accessed via proxy. The only option available is to block access to anonymous proxies entirely to prevent potential access to CSA content.
This is not a mandatory requirement. In case there is not possibility to differentiate between CSA content and other content, then blocking access to anonymous proxies is not required.

**Q18:** The current bid requires the installation of the solution under section 4 – *"Install, test, commission and maintain the cloud-based CSA filtering solution".* Given the current and future travel restrictions due to Covid-19, is an on-site visit a mandatory requirement? Should any installation be required in-country, can this be performed remotely?
Yes, remote installation is acceptable

**Q19:** Further to the above question, can training be completed remotely (i.e. via remote sessions)?
Yes

**Q20:** Please confirm that English, Thai, Arabic, Bahasa Indonesia, Vietnamese, Chinese, Urdu are required to be filtered for the following categories and that the intention is to block the following categories: *Pornography*, Child Pornography, Gambling, Drug Abuse, Online Sales, Extreme, Hate Speech, Malware, Virus, Phishing, Web proxy anonymizers.
Multilanguage filtering is required for child pornography online content only