Mozilla Corporation
331 E. Evelyn Ave.
Mountain View, CA 94041

June 23, 2015

Honorable Fred Upton
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

Dear Chairman Upton and members of the Committee,

Thank you for your letter dated June 9, 2015. We are excited to see your interest in the security and stability of the Web — it is something that we see as central to our work as well.

We are a mission-driven company grounded in the beliefs embodied in the Mozilla Manifesto,[1] and in the history of the broader Open Source project that encompasses our work. Our products are built to serve our users through our mission, including the Firefox browser (desktop and mobile), our cloud services products, and the Firefox OS mobile operating system. In addition, we invest considerable time and resources advancing our mission through policy. Our root Certificate Authority (CA) program is one of our many projects that combines both. It is grounded in transparency and objectivity, as articulated in the Mozilla Root CA Certificate Policy[2] (specifically, the inclusion section;[3] emphasis added):

> "We will determine which CA certificates are included in software products distributed by Mozilla, based on the **benefits and risks of such inclusion** to typical users of those products. … We will make such decisions through a **public process**, based on **objective and verifiable criteria**..."

Openness and transparency are central to Mozilla, and are especially important when it comes to the root CA program because of the trust that users put in that program. To maintain that trust, all changes to the Mozilla root certificate program are made through our open process.

The question of whether government CAs should be restricted to issue only certificates within their ccTLDs is currently under discussion[4] on the public Mozilla security policy mailing list.[5] Our process is

[1] https://www.mozilla.org/en-US/about/manifesto/
[2] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
[3] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/
[4] https://groups.google.com/d/topic/mozilla.dev.security.policy/tr_PDVsZ6-k/discussion
[5] https://groups.google.com/forum/#!forum/mozilla.dev.security.policy

not complete and thus we have not come to any decisions. We encourage you to review that discussion, as it includes substantial information about the benefits and risks of such a proposal.

Although we have not yet concluded our process, this letter reflects what we have learned through our public analysis and discussions so far. We are concerned that mandatory scope restrictions on any CAs, including government CAs, would present many challenges with uncertain benefits. We recognize the potential benefits of constrained CAs for security, and in fact, the Mozilla Root CA Certificate Policy today encourages all CAs to restrict themselves to issuing certificates for their own respective properties (to be "technically constrained" in the words of the policy). However, converting this existing best practice into a binding requirement, either for all CAs or for any sub-category such as government-run CAs, could introduce many short- and long-term problems.

With regard to the specific questions in your letter:

> *1. Would restricting CAs run by governments to issuing certificates for their own properties within their ccTLDs improve the security and stability of the certificate ecosystem? If so, how? If not, why not?*

Constraining CAs can be beneficial from a security standpoint, as it reduces the harm that the constrained CA can cause (regardless of whether the CA is run by a government). However, new constraints can hurt stability by forcing CAs to change their operations, or forcing software developers to update constraints as needs change.

Restricting government CAs to their own properties in their respective ccTLDs would not be compatible with the operational models of several existing government CAs. There are government CAs in Spain and Taiwan that issue certificates to individuals and business as well as government organizations. There are also government CAs that issue only to government organizations, but outside of their ccTLD. For example, the Catalan CA CATCert has issued a certificate for https://orgt.mobi, which is used by the provincial council for Barcelona — indeed, CATcert's own website is https://www.catcert.net. The US Federal PKI root (not currently included in the Mozilla root store) has issued a certificate for https://cyberfetch.org (not a .gov or .us domain), a Department of Homeland Security project.

Unconstrained CAs have the ability to issue fraudulent certificates, whether they are run by governments or by other entities. But it's unclear whether constraints on government CAs would be an effective measure to address this problem. For example, governments could compel commercial CAs within their legal jurisdiction to issue bad certificates. Thus, constraining one CA or a class of CAs may not in practice reduce the scale of fraudulent certificate issuance.

> *2. Is it currently technically feasible to restrict government CAs to their own properties in their respective ccTLDs? (2.A.) If so, how would this change be implemented? (2.B.) If not, what technological barriers exist? Could these barriers be removed or mitigated?*

In general, it is technically feasible to restrict government CAs to their respective ccTLDs, but there are significant technical challenges to restricting them to their own *properties*. As discussed in the previous

answer, many government properties use names that fall outside of the .gov equivalents — indeed, outside of the respective country's ccTLDs — so a restriction to ccTLDs would be a poor match for current naming practices and could introduce substantial instability for many legitimate use cases.

Implementing a restriction that aligns to existing naming practices would be more challenging. To do so, we would need to collect a list of the domain names allowed for each government CA and vet that list to ensure that each allowed name actually corresponds to a government-operated site. Additionally, browsers would need to be configured to keep an up-to-date copy of this list (since it will change over time), and to reject certificates issued by government CAs that are not allowed by the list.

Accurately restricting government CAs to their respective properties through such a list would likely require more labor than is used to maintain the entire CA program today. Furthermore, although ordinary operation of a root store involves some similar technical challenges, such as providing browsers an up-to-date list of revoked certificates, adding additional layers of complexity to this system increases its instability and risk.

> *3. Are there any potential negative effects to such a restriction? If so, please describe them.*

For the many practical reasons described above, the imposition of constraints on government CAs would risk significant harm to stability, with little clear security benefit. As noted above, the government CAs currently in the Mozilla root store have issued many certificates for web sites outside of their ccTLDs. If government CAs were to be restricted to issuing certificates for their own properties in their ccTLDs, then these certificates would have to be revoked, and website owners would have to acquire a certificate from a different CA. Alternatively, browsers would be required to keep a whitelist of certificates that are "grandfathered in," which would pose similar technical challenges to those discussed in Question 2.

At a higher level, if any restrictions are imposed outside of established processes that drive the certificate ecosystem, such as our community process (e.g., through regulation), it could potentially undermine user trust in the certificate ecosystem as a whole. It is critically important for the stability, security, and fundamental utility of the certificate ecosystem that users trust the administration of the browsers' root CA programs. We maintain that trust by making decisions through our open, community driven processes, grounded in our principles. The question of how root CA programs should treat government CAs is a complex issue that requires global, multi-stakeholder discussion. Any action by any individual government, outside of that framework, would be harmful to the stability of the certificate ecosystem by undermining users' trust in it.

> *4. If the restriction of government CAs to their own properties in their respective ccTLDs would not improve the security and stability of the certificate ecosystem, are there policies or technologies that would? If so, please describe them.*

As we said above, the Mozilla root CA program is based on openness. When CAs are open about their operations, it enables the community to verify that the CA's operations are compliant with the

commitments it has made to the community (increasing trust in the system), and it allows browsers to reject certificates that the CA may have issued in error (increasing the security of the system).

Mozilla is advancing openness by requiring that CAs disclose all non-constrained subordinate CA certificates, a policy we developed through our own open mechanisms for community-grounded discussion. In addition to allowing the community to better gauge the risks posed by CAs, this disclosure requirement could also allow browsers to reject certificates issued by non-disclosed CAs. Since many of the major mis-issuance incidents in the recent past have involved non-disclosed CAs, there is clear benefit to being able to recognize non-disclosed CAs and reject certificates that they have issued.

***

We would like to close by thanking the Committee again for your interest. If there is anything else Mozilla can provide, please contact me.

Sincerely,

_____

Denelle Dixon-Thayer
General Counsel and Senior VP for Public Policy
Mozilla

cc: Chris Riley, Head of Public Policy <criley@mozilla.com>
Richard Barnes, Firefox Security Lead <rbarnes@mozilla.com>