ICANN BOARD SUBMISSION No. 2015.04.26.2g - Rev 1

TITLE: **Funding for Digital Services platforms and code-base review**

PROPOSED ACTION: **For Board Approval**

EXECUTIVE SUMMARY:

ICANN delivers a portfolio of 85 digital services for the benefit of its served communities. These services have been developed and placed in service over the last 15 years, leveraging some 10+ different software platforms. The inherent software code-base security of all these services needs to be confirmed. Such a comprehensive assessment by an external subject matter expert firm/s was not contemplated during the 2015 budget cycle, but it is important to begin this process before the start of FY16. Since this exercise was not specifically budgeted for, and it is anticipated that this exercise will entail an investment of over US$500,000, any such expenditure must be approved by the Board. Further, a long-term view of sec urity requires a comprehensive look at both systems design and systems architecture to ensure that security thinking is at the forefront of decision making. The Reference Materials for this paper summarize the steps taken thus far, and outlines the proposed next steps.

STAFF RECOMMENDATION:

Staff recommends that the Board delegate to the President and CEO, or his designee(s), the authority to take all actions necessary to obtain a comprehensive review and security vulnerability assessment of all software platforms in use at ICANN for delivering digital services, including contracting with external service providers, acquiring needful tools and expenditure disbursement.

BOARD RISK COMMITTEE RECOMMENDATION:

The Board Risk Committee recommends that the Board delegate to the President and CEO, or his designee(s), the authority to take all reasonable actions necessary to obtain a comprehensive security vulnerability assessment of all software platforms in use at ICANN for delivering digital services, including contracting with external service providers, acquiring needful tools and

expenditure disbursement. The BRC further recommends that the CEO or his designee provide regular updates to the BRC regarding progress on a plan to ensure systems design and systems architecture are integrated into standard ICANN processes, and that security considerations occupy an essential role in corporate decision making.

BOARD FINANCE COMMITTEE RECOMMENDATION:

The Board Finance Committee recommends that the Board delegate to the President and CEO, or his designee(s), the authority to take all reasonable actions necessary to obtain a comprehensive security vulnerability assessment of all software platforms in use at ICANN for delivering digital services, including contracting with external service providers, acquiring needful tools and expenditure disbursement.

PROPOSED RESOLUTION:

Whereas, staff has compiled a complete list of all digital services offered by ICANN to its served communities.

Whereas, ICANN offers a total of 85 such digital services, some 50 of which are services that have been partially or wholly developed by ICANN staff, or under ICANN staff supervision, leaving a code-base for maintenance under ICANN staff control.

Whereas, the Board Risk Committee has reviewed preliminary findings as presented by the Chief Innovation and Information Officer (CIIO) during ICANN52 in Singapore.

Whereas, the Board Risk Committee has reviewed the CIIO's short- and longer-term treatment of IT security matters on 17 April 2015.

Whereas, the Board Finance Committee has recommended that the Board delegate to the President and CEO, or his designee(s), the authority to take all actions to address the immediate need of assessing the software code-base managed by ICANN staff

Resolution Text Superseded

Resolution Text Superseded

Whereas, there are sufficient funds in the FY15 contingency fund to cover the costs of this project.

Resolved (2015.04.26.xx), the Board authorizes the President and CEO, or his designee(s), to

Resolution Text Superseded

Resolved (2015.04.26.xx), the Board directs the President and CEO, or his designee(s), to provide regular updates to the Board Risk Committee on the progress of the long-term plan to ensure systems design and systems architecture are integrated into standard ICANN processes, and that security considerations occupy an essential role in corporate decision making.

Resolution Text Superseded

PROPOSED RATIONALE:

As part of ICANN's digital services health-check, during summer of 2014, ICANN's IT organization initiated an RFP process to select a suitable external third-party with a reputation and the needful skills to assess all the services and the underlying technologies ICANN has deployed. Following the RFP process, ICANN selected and engaged the services of a globally-recognized leader in undertaking such assignments.

The selected contractor performed a thorough analysis of the ICANN portfolio of digital services. Jointly, ICANN staff and the contractor decided to leverage the SANS Institute 20-factor Critical Security Controls framework. The contractor produced a report in late Summer 2014 to identify those framework-factors that met or exceeded the "Green" standard, while also identifying those framework-factors that could use further attention.

The report particularly highlighted one factor – Application Software Security – for deeper analysis.

Concurrently, staff inventoried all the digital services it offers the ICANN community. That number stands at 85 today. Staff catalogued the number of software platforms (development environment plus database or content management system), which have been leveraged to develop these services over the last 15+ years. Staff also determined that ICANN delivers digital services leveraging 10+ software platforms for the benefit of its served communities.

Following the SANS Institute framework-based assessment, ICANN IT staff initiated a 16-projects portfolio, focused on improving ICANN's defences in those IT infrastructure areas meriting further attention.

Staff analysed the nature of data captured, manipulated, stored and delivered by these services. The analyses looked at data integrity, data sensitivity and data privacy, among other factors. The result of this analysis showed a concentration of high-sensitivity data in services that serve ICANN's Contracted Parties community.

Staff retained the services of a deep-specialty firm with expertise in the software package and platform utilized by ICANN to specifically assess digital services deployed for the benefit of the New gTLD program. This specialty firm produced a report in late February of 2015, identifying areas that merited further attention.

Staff has determined that all other (~10) software platforms merit similar assessments. In attempting to estimate the costs of this project, staff approached three large firms with extensive ranges of skill sets and knowledge on numerous software platforms. Staff then also made cost inquiries at smaller, niche or subject matter expert firms that have concentrated expertise on just one or a few software platforms. The estimates received from the larger firms were significantly higher than those from the niche firms, even though both size firms have relatively equal expertise on any given software platform for which the niche firms have concentrated expertise. Accordingly, staff appropriately determined to recommend using numerous, smaller niche firms, rather than one larger firm for this project.

The Board reviewed staff's recommendation for assessing potential software-driven vulnerabilities in the code-base of services leveraging these platforms, and the determination that the proposal met the standard for such assessments. The process for selection of subject matter expert firms for such assessments does not call for public consultation, as the assessment of the code-base is the primary consideration and the spend with any given vendor is not expected to reach the level requiring a public bidding process as set out in ICANN's Procurement Guidelines (see https://www.icann.org/en/system/files/files/procurement-guidelines-21feb10-en.pdf).

There will be a financial impact on ICANN in engaging in such an assessment, and given that it was not previously specifically budgeted and that it is above management approval levels, staff has come to the Board for approval.

This is an Organizational Administrative function that does not require public comment.

Submitted by:	Ashwin Rangan
Position:	Chief Innovation & Information Officer
Date Noted:	09 April 2015
Email	ashwin.rangan@icann.org