Implementation Recommendations for SSAC Advice Document SAC074

SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

Recommendation	Description	ICANN's Statement of Understanding	Background on the Issue	ICANN Organization Implementation Recommendation & proposed implementation plan	Rationale for Implementation Recommendation
1	As part of regular reports, the ICANN Compliance Department should publish data about the security breaches that registrars have reported in accordance with the 2013 Registrar Accreditation Agreement (RAA), paragraph 3.20.	*ICANN's Contractual Compliance department should provide regularly updated data about security breaches reported in accordance with the 2013 Registrar Accreditation Agreement (RAA), paragraph 3.20. This data should include statistics about the number of security breaches, the number of registrars affected, the aggregate number of registrants affected, and the high-level causes of the breaches. The SSAC does not recommend at this time whether specific registrars' names should be published.*	The SSAC advisory states, *attacks that compromise registrant data and/or the DNS settings of domain names continue to be a significant problem for registrars and registries, as well as for the registrants themselves and the users of their sites.* The 2013 Registrar Accreditation Agreement (RAA) requires registrars to disclose certain information regarding security breaches to ICANN Contractual Compliance. Having ICANN org provide appropriately anonymized reporting regarding security breaches at Registrars will be a useful way to provide better information to the Registrar community as to the nature of the threat landscape.	Implementation is recommended.

The Contractual Compliance department will add the requested data to its existing public reporting. | This request is within the remit of the ICANN Org and the data is available to the organization based on the provisions in the 2013 RAA. The Contractual Compliance team has the data tools, and resources necessary to publish the requested reporting. Implementation can be achieved with the existing FY19 Budget for the Contractual Compliance department. |
| 2 | A provision similar to paragraph 3.20 of the 2013 Registrar Accreditation Agreement (RAA) should be incorporated into all future gTLD Registry Agreements, with similar statistics published (e.g., about the number of breaches, the number of registrars affected, the aggregate number of | Our understanding of this advice is that a provision similar to paragraph 3.20 of the 2013 Registrar Accreditation Agreement (RAA) should be incorporated into all future gTLD Registry Agreements, with similar statistics published (e.g., about the number of breaches, the number of registrars affected, the aggregate | The Registrar Accreditation Agreement contains provisions that require Registrars to report information to ICANN regarding breaches to their systems, but the Registry Agreement does not. The SSAC is identifying this gap, and requesting ICANN to require Registry Operators to do the same level of | Implementation will be attempted.

The ICANN Org will include this in the proposed changes to the registry agreement during the next bilateral negotiation. | The SSAC advises this requirement will contribute to better security and stability in the DNS. Ensuring and improving the security and stability of the DNS is within ICANN's remit. There would be no impact to the budget to pursue the proposed implementation plan. |

Recommendation	Description	ICANN's Statement of Understanding	Background on the Issue	ICANN Organization Implementation Recommendation & proposed implementation plan	Rationale for Implementation Recommendation
	registrants affected, and the high-level causes of the breaches).	number of registrants affected, and the high-level causes of the breaches).	reporting and disclosure regarding any system breaches.		
3	Future RAA deliberations should encourage stronger authentication practices, specifically the use of multi-factor authentication	Our understanding of this advice is that for future versions of the Registrar Accreditation Agreement (RAA), ICANN should advocate that registrars are committed to stronger authentication practices than those which they are committed to in the 2013 RAA, specifically the use of multi-factor authentication.	The SSAC advisory states, attacks that compromise registrant data and/or the DNS settings of domain names continue to be a significant problem for registrars and registries, as well as for the registrants themselves and the users of their sites. The advisory goes on to say *Multi-Factor authentication remains a key element in efforts to establish a more secure environment.* Their recommendation is to encourage stronger authentication practices by registrars, and to consider doing so via the RAA.	Implementation will be attempted. ICANN Org will request the Registrars to consider contractual requirements relating to the authentication practices of registrants in a future round negotiation of the Registrar Accreditation Agreement.	The SSAC advises that multifactor authentication will contribute to enhanced security and stability for registrants and thus the DNS. Ensuring and improving the security and stability of the DNS is within ICANN's remit. There would be no impact to the budget to pursue the proposed implementation plan.
4	The ICANN Board should direct ICANN staff to facilitate global hands-on training programs for registrars and registries based on the best practices outlined in Section 6 of this document, with the goal to enable parties to learn practical operational practices for preserving security and stability of the credential management lifecycle.	Our understanding of this advice is that ICANN staff should facilitate training programs for registrars and registries relating to the credential management cycle. These trainings should focus on the best practices outlined on SAC074. We note the SSAC's offer to provide input to ICANN's development of the training curriculum.	The SSAC advisory goes into significant detail of the credential management lifecycle in the registry, registrar, registrant ecosystem, and provides a series of best common practices. They advice ICANN to develop and provide hands on training for registries and registrars on these practices in the name of registrant protection.	Implementation is recommended. The Global Domains Division will provide the requested training. The training would likely occur at a future GDD Summit or ICANN meeting and be recorded for future use.	The purpose of Global Domains Division (GDD) is to serve the global public interest, the registrants and end users of the Internet by ensuring a secure and stable domain name system (DNS), while promoting trust, choice, and competition in the trusted domain name service industry. Providing training to the contracted parties to help protect registrants is consistent with the stated purpose of the GDD. The training can be developed and provided by prioritizing the activity with the existing FY19 Budget request.