Attachment 30A-2: SSWG Enhanced Security Standards

	Standard	Control	Rationale	Notes
1.	Registry Operator must define and implement a name selection policy (i.e., what types of names may be registered.)	Registry Operator must provide an adequate description of its name selection policy.	Ensure domains are compliant with the name selection policy.	This standard must be applied to all new gTLDs[1] (i.e., standard and community applications) that perform financial services[2] activities. Footnotes 1 and 2 apply to all standards.
2.	Registry Operator must define and implement a name allocation policy inclusive of a process to resolve a conflict between identical or confusingly similar names.	Registry Operator must provide an adequate description of its name allocation policy inclusive of a process to resolve contention between or among names.	Ensure domains are compliant with naming allocation policy and that contention is resolved according to pre-published methods.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities.
3.	Registry Operator must define and implement a registrant eligibility requirements policy.	Registry Operator must provide an adequate description of its registrant eligibility requirements policy.	Ensure domains are compliant with eligibility requirements.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities. For example, a registrant in the .bank TLD must be a licensed/registered bank as defined by the banking laws of the regulatory authority in the relevant jurisdiction.

[1] The proposed standards may not apply to branded gTLDs. Branded gTLDs are however strongly encouraged to adopt as many of the recommendations as feasibly possible.

[2] Financial services are activities performed by financial institutions, including: (1) the acceptance of deposits and other repayable funds; (2) lending; (3) payment and remittance services; (4) insurance or reinsurance services; (5) brokerage services, including money brokering; (6) investment services and activities, including underwriting of securities, market-making, and dealing in securities and other financial products; (7) financial leasing; (8) issuance of guarantees and commitments; (9) provision of financial advice; (10) portfolio management and advice; or (11) acting as a clearinghouse. To avoid doubt, a person’s conduct is not the provision of a financial service if it is done in the course of work of a kind ordinarily done by clerks or cashiers.

	Standard	Control	Rationale	Notes
4.	Registry Operator must define and implement a content and acceptable use policy for registrants.	Registry Operator must provide an adequate description of its content and acceptable use policy for registrants.	Ensure domains are compliant with content and acceptable use policy.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities.
5.	Registry Operator must define and implement a policy for amending its registration requirements.	Registry Operator must provide an adequate description of the process it will undertake to amend its registration policies (i.e., name selection, name allocation, eligibility requirements, content and acceptable use).	Ensure there is support for the proposed policy changes and that they are consistent with the spirit under which the TLD was granted.	This standard must be applied to all new gTLDs (i.e., standard and community applications) that perform financial services activities. Registry Operators of community TLDs may also be subject to ICANN's gTLD Community gTLD Change Request Handling Process available in draft form at http://www.icann.org/en/topics/new-gtlds/explantory-memo-community-change-request-21feb11-en.pdf.
6.	Registry Operator must certify annually to ICANN its compliance with its Registry Agreement.	Registry Operator must provide an adequate description of its proposed certification process.	Ensure Registry Operator is compliant with its Registry Agreement.	The certification process could include an independent, third-party audit, an officer's attestation, etc.
7.	Registrar must certify annually to ICANN and Registry Operator, respectively, its compliance with its Registrar Accreditation Agreement and Registry-Registrar Agreement.	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar to annually certify compliance with their Registry-Registrar Agreement and their Registrar Accreditation Agreement.	Ensure Registrar is compliant with its Registrar Accreditation Agreement and its Registry-Registrar Agreement.	Compliance for Registrar could be identical or similar process for Registry Operator.

	Standard	Control	Rationale	Notes
8.	Registry Operator must provide and maintain valid primary contact information (name, email address, and phone number) on their website.	Registry Operator must provide an adequate description of how and where it will present such information on its website.	Ensure Internet users are able to reach a primary contact to resolve an issue.	Registry Operator is encouraged to provide contact information for other functions, including but not limited to, abuse, compliance, operations, technical, etc.
9.	Registrar must provide and maintain valid primary contact information (name, email address, and phone number) on their website.	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar compliance with this policy.	Ensure Internet users are able to reach a primary contact to resolve an issue.	Registrar is encouraged to provide contact information for other functions, including but not limited to, abuse, compliance, operations, technical, etc.
10.	Registry Operator must re-validate its Registry-Registrar Agreements at least annually.	Registry Operator must provide an adequate description of its re-validation process to include an action plan if Registrar fails re-validation and cannot cure the failure.	Ensure that Registrars continue to meet the requirements defined in the Registry-Registrar Agreement.	
11.	Registry Operator must provide and publish an elevated service capability with a well-defined escalation process to acknowledge and respond to an emergency.	Registry Operator must provide an adequate description of its elevated service capability and its escalation process and both once finalized are to be published on their website.	Ensure that during an emergency the Registrar (and in some cases Registrants and other users) can escalate their issue with the Registry Operator.	An elevated service capability must include 24/7 365 customer service.

	Standard	Control	Rationale	Notes
12.	Registrar must provide and publish an elevated service capability with a well-defined escalation process to acknowledge and respond to an emergency.	Registry Operator must include in its Registry-Registrar Agreement that Registrar must provide an elevated service capability and an escalation process and both once finalized are to be published on their website.	Ensure that during an emergency the Registrant (and in some cases other users) can escalate their issue with the Registrar.	An elevated service capability must include 24/7 365 customer service.
13.	Registry Operator must notify Registrar immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN or any outside party (e.g., law enforcement, etc,).	Registry Operator must provide an adequate description of its notification process including under what circumstances notice may not be required.	Ensure that Registry Operator adheres to high standards of integrity in operations, accountability, and transparency. The requirement to report an investigation or compliance action could be included in its Registry Agreement with ICANN.	
14.	Registrar must notify Registry Operator immediately regarding any investigation or compliance action including the nature of the investigation or compliance action by ICANN along with the TLD impacted.	Registry Operator must include in its Registry-Registrar Agreement a description of its notice requirements and the circumstances, if any, when notice may not be required.	Ensure that Registrar adheres to high standards of integrity in operations, accountability, and transparency.	

	Standard	Control	Rationale	Notes
15.	Registry Operator must explicitly define for Registrars what constitutes abusive conduct including, but not limited to, malicious, negligent, and reckless behavior. The defined permissible frequency and the course of action in cases of repeated violations must be provided.	Registry Operator must include in its Registry-Registrar Agreement the definitions of abusive conduct including, but not limited to, malicious conduct, negligence, and reckless behavior including the defined permissible frequency and consequences of such behavior.	Ensure that Registrars are fully informed of the definition and consequences of irresponsible behavior.	
16.	Registry Operator must explicitly define for Registrants what constitutes abusive conduct including, but not limited to, malicious, negligent, and reckless behavior. The defined permissible frequency and the course of action in cases of repeated violations must be provided.	Registry Operator must include in its Registry-Registrar Agreement a requirement that Registrar include in its Registration Agreement a definitions of abusive conduct including, but not limited to, malicious conduce, negligent, and reckless behavior including the defined permissible frequency and the consequences of such behavior.	Ensure that Registrants are fully informed of the definition and consequences of irresponsible behavior.	
17.	Registrar with significant compliance infractions will be ineligible to provide registration services to a TLD with elevated security requirements.	Registry Operator must include in its Registry-Registrar Agreement an adequate description of the consequences of significant compliance infractions.	Ensure that Registrars with an excellent track record in operations are eligible to serve the TLD.	

	Standard	Control	Rationale	Notes
18.	Proxy registrations are prohibited.	Registry Operator and Registrar must communicate the proxy registration prohibition and include contractual language about it in the Registry-Registrar Agreement and Registrant Registration Agreement.	Ensure transparency for all registrations.	
19.	Registrar must disclose registration requirements on their website.	Registry Operator must include in its Registry-Registrar Agreement a requirement that Registrar must disclose registration requirements on their website.	Ensure that Registrants understand the requirements so they may successfully complete the registration process.	
20.	Registry Operator must ensure that vendors who provide services to Registry Operator and Registrar are obligated to meet the applicable TLD policies.	Registry Operator must provide an adequate description of how it will ensure its vendors, and the vendors of its Registrars, may comply with the TLD policies.	Ensure that third-party service providers are thoroughly vetted and vulnerabilities with said providers are addressed through technical and operational processes.	

	Standard	Control	Rationale	Notes
21.	In the event of transition from one Registry Operator to another, the successor Registry Operator must agree to abide by all policies and procedures that have been implemented prior to the time of transition.	N/A	Ensure that once a TLD is operated with elevated security standards that it continues to be regardless of the Registry Operator.	ICANN’s Explanatory Memorandum on gTLD Registry Transition Processes is available at http://www.icann.org/en/topics/new-gtlds/registry-transition-processes-clean-30may11-en.pdf.
22.	Domain names will not be activated or resolve in the DNS until they have been validated against the eligibility and name selection policies.	Registry Operator must provide an adequate description of its validation process to include the milestone for domain name activation.	Ensure the legitimacy of registrations prior to activation.	
23.	Registry Operator (or Registrar depending on the validation process) must re-validate at least semi-annually that Registrant Whois is 100% accurate.	Registry Operator must provide an adequate description of how data will be re-validated or how the re-validation requirement might be passed on to its Registrar. An affirmative confirmation by the Registrant is required for the re-validation to be considered complete. If the Registrant fails to respond an escalated review a notification process will be initiated.	Ensure there will be an ongoing validation of registration data so that Registrant Whois is 100% accurate.	

	Standard	Control	Rationale	Notes
24.	The Registry Operator must ensure that technical implementations do not compromise elevated security standards.	Registry Operator must provide an adequate description of its policy to ensure elevated security levels are not compromised during the implementation of new technology.	Ensure that elevated security standards are maintained and preserved during the implementation of any new registry feature, service, etc.	
25.	The Registry Operator, Registrar, and Registrant must establish digital assertion during the registration process.	Registry Operator must provide an adequate description of its policy for digital assertion using best current practices and how that requirement will be applied to Registrars and Registrants.	Ensure digital identity can be verified and trusted for communication between parties.	Best current practices do not include self-signed certificates.
26.	DNSSEC must be deployed at each zone and subsequent sub-zones. Registrar and Registrant must deploy DNSSEC with each domain name at launch (to compliment ICANN requirement for Registry Operator).	Registry Operator must include in its Registry-Registrar Agreement the requirement for Registrar deployment of DNSSEC. Registrar must communicate the DNSSEC requirement to Registrant in Registration Agreement.	Ensure DNSSEC is deployed all levels within a zone to establish the chain of trust for domain names in the TLD.	
27.	Registrar access to all Registry systems must be mutually authenticated via Transport Layer Security and secured with multi-factor	Registry Operator must provide an adequate description of their authentication processes and include in its Registry-Registrar Agreement a	Ensure security and provide additional evidence of the requesting entity's identity to the receiving entity.	

	Standard	Control	Rationale	Notes
	authentication, NIST Level 3 or better.	comparable provision.		
28.	Registrant access to all Registrar systems must be mutually authenticated via Transport Layer Security and secured with multi-factor authentication, NIST Level 3 or better.	Registry Operator must provide an adequate description of their requirement for Registrant and Registrar authentication processes and include in its Registry-Registrar Agreement and Registration Agreement a comparable provision.	Ensure security and provide additional evidence of the requesting entity's identity to the receiving entity.	
29	Registry Operators, Registrars, and Registrants are required to use encryption practices that have a 30-year or longer security strength time frame as defined by NIST Special Publication 800-57, or its successor, for electronic communication between parties, including but not limited to web access, mail exchange, and file transfer, avoiding the use of unencrypted protocols in order to prevent the tampering of critical messages containing credentials or sensitive information.	Registry Operator must include this requirement in its Registry-Registrar Agreement and Registrar must include the same in their Registration Agreement.	Ensure security of communication over the Internet to prevent eavesdropping, data tampering, etc.	

	Standard	Control	Rationale	Notes
30.	Registrants must publish valid Email Authentication records in the DNS space for all active domains and sub-domains. These records include Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and any tools or technologies that improve or replace these protocols.	Registry Operator must include in its Registry-Registrar Agreement that Registrar's Registration Agreement must specify this requirement.	Ensure security by preventing the delivery of invalid or spoofed email purporting to be from a particular domain.	
31.	DNS Resource Records: 1. CNAME and DNAME are prohibited from aliasing DNS records outside of the secure zone. 2. Nameserver host names must be in the parent zone.	Registry Operator must provide an adequate description of their DNS Resource Records requirements.	Ensure traditional DNS zones may not impersonate higher security DNS zones.	2. Example: finame.bank NS => ns1.finame.bank, ns2.finame.bank or perhaps ns1.ultradns.bank or ns1.dyndns.secure or the like. NOT finame.bank => ns1.finame.biz or ns2.ultradns.biz.