2016 Security Requirements:

What Service Providers Need to Know

June 9, 2016

fTLD Registry Services, LLC

Webinar Guidelines

- All participants will be muted
- Questions can be posed via questions box
  - Will be consolidated for Q&A at the end
  - May be submitted to fTLD@fTLD.com after the webinar
  - fTLD may compile a FAQ from the webinar
- You can participate via audio through your computer or by using the dial-in details provided with your registration confirmation
- Recording and presentation will be shared with participants and posted on fTLD's websites

Program

- History
- About the 2016 Security Requirements
- Who may help meet the Security Requirements
- Ways to meet the Security Requirements
- Changes to the Security Requirements
- Universal Acceptance
- Resources
- Questions

History

- fTLD Registry Services – formed in 2011 to serve and protect the global banking and insurance communities
- Awarded the right to administer .BANK in September 2014 and .INSURANCE in February of 2015
- Operating trusted, verified, more secure and easily identifiable locations online for the sectors and their customers
- fTLD has:
  - Eligibility Requirements
  - Verification Requirements
  - Security Requirements
  - Monitoring and Compliance of all Requirements

History (cont'd.)

- 2011: Community-based Security Standards Working Group developed first standards
- 2013-14: fTLD commenced engagement with industry service providers
- 2014: Community-based Security Requirements Working Group proposed modifications; reviewed by fTLD Advisory Council and approved by fTLD Operating Manager and Board of Directors

History (cont'd.)

- 2015: Community feedback about implementation challenges:
  - Not all service providers are ready to support requirements in time
  - Requirements were impacting common security and resiliency controls
  - Registrants use third-party utility services with domain names that are not .BANK

- 2015-16: Security Requirements Working Group reconvened to consider modifications; reviewed and approved as in 2014

About the 2016 Security Requirements

- Does not materially change anything for .BANK and .INSURANCE domain names
- Defined Services (i.e., hosted email solutions, content delivery networks, security/fraud services and aliasing to legacy domains) may be delivered from non-.BANK and non-.INSURANCE domain names
  - fTLD Security Requirements, including monitoring and compliance program, extended to these domain names
- Redirection clarified and incorporated
- Compliance exemption in Emergency Situations
- Specifies implementation schedule for certain requirements for non-.BANK and non-.INSURANCE domain names

Who may help meet the Security Requirements

- fTLD-approved Registrars
- Website hosting provider
- Service provider (e.g., core processor, content delivery networks)
- DNS service provider

Note: fTLD may add a resource page to its websites to identify providers that can meet the Security Requirements

Ways to meet the Security Requirements

- Historically two-options:
  - Service provider registers a .BANK or .INSURANCE domain name
  - Registrant delegates a .BANK or .INSURANCE third-level domain name to service provider (e.g., serviceprovidername.bankname.bank)

- 2016 modifications enable delivery of Defined Services from non-.BANK and non-.INSURANCE domain names

Changes to the Security Requirements

Authorizations for Defined Services Deployed on Non-.BANK or Non-.INSURANCE Domains

Requirements/ Defined Services	#23 – DNSSEC	#25 & #29 - TLS/Encryption Practices	#26 - Email Authentication	#27 - DNS Resource Record Restrictions
Hosted Email Solutions	Required by January 1, 2018	Required for Email and Web Services Only Required by April 1, 2017		Exceptions for CNAME and MX
Content Delivery Networks	Required by January 1, 2018		N/A	Exception for CNAME
Security* and Fraud Services	Required by January 1, 2018		N/A	Exception for CNAME
Aliasing to Legacy Domains				Exception for CNAME

Key: Green – fTLD Security Requirements apply now
Yellow – Delayed implementation of fTLD Security Requirements
Red – Enduring changes to fTLD Security Requirements
Orange – N/A (Not Applicable)

* The Security Requirements do not apply to Distributed Denial of Service mitigation services that do not use DNS Resource Records within the .BANK or .INSURANCE Domain Name System.

Requirement #23

- Domain Name System Security Extensions (DNSSEC) ensures that Internet users are landing on legitimate websites and not being misdirected to malicious ones
- No change for .BANK and .INSURANCE domain names
- Select Defined Service delivered from non-.BANK or non-.INSURANCE domain names must be compliant by January 1, 2018
- Legacy domains (e.g., .COM, .NET) must implement DNSSEC if they are to alias to .BANK or .INSURANCE (e.g., website mirroring)

Requirements #25 & #29

- Transport Layer Security ensures confidentiality and integrity of communications over the Internet. Transport Layer Security 1.1 or greater must be used. Any version of SSL is explicitly prohibited as is TLS 1.0.
- No change for .BANK and .INSURANCE domain names
- Hosted email solutions delivered from non-.BANK or non-.INSURANCE domain names must be compliant by April 1, 2017
- For all other Defined Services, compliance is required at deployment

Requirement #26

- Email Authentication protects brands by mitigating spoofing, phishing and other malicious email borne activities
- No material changes for .BANK and .INSURANCE domain names
- For hosted email solutions delivered from non-.BANK or non-.INSURANCE domain names or used in aliasing to legacy domains, compliance is required at deployment

Requirement #26 (cont'd.)

- Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - Identifies if the domain is used for sending email
  - One policy can be set to govern all child domains (if appropriate)

- If the domain is not used for sending email (e.g., a parked domain), basic DMARC record is required (i.e., p=reject)

- If domain name is used for sending email, must deploy:
  - Domain Keys Identified Mail (DKIM): allows the receiver to check that an email claimed to come from a specific domain was indeed authorized by the owner of that domain; **or**

  - Sender Policy Framework (SPF): list of authorized host names/IP addresses that can send mail for the domain

- For best results, deploy DKIM and SPF with DMARC

Requirement #27

- Domain Name System (DNS) Resource Records (e.g., CNAME, MX) were previously prohibited from aliasing to non-.BANK and non-.INSURANCE domain names

- There are now exceptions for Defined Services and specific DNS Resource Records, subject to compliance with certain requirements:
  - Hosted email solutions: CNAME and MX
  - Content delivery networks: CNAME
  - Security and fraud services: CNAME
  - Aliasing to legacy domains: CNAME

Requirement #30

- Redirection away from .BANK and .INSURANCE domain names is permissible as follows:
  - Access to secure services (e.g., online banking, transactional operations) is subject to compliance with requirements 23*, 25, 26 and 29
  - Access to third-party content (e.g., affiliates, blogs, social media) is not subject to compliance with the requirements
  - Use of “speed-bumps” is strongly encouraged

* Must be compliant by January 1, 2018; #25, #26 and #29 are required at deployment

Requirement #31

- Registrant compliance waiver with requirements 23, 25, 26, 27, 28, 29 and 30 in Emergency Situations
- Registrant is required to provide written notice to fTLD (online form to be available ~July 1, 2016)
- Emergency Situations are defined as present or imminent events such as:
  - Incidents that threaten systematic security, stability and resiliency of registrant infrastructure;
  - Unauthorized access to or disclosure, alteration, or destruction of registrant data or that of its customers;
  - An occurrence with the potential to cause a failure of registrant infrastructure.

Universal Acceptance

- The issue: some applications do not yet recognize new Internet web extensions; domain names or email addresses

- What is being done about it?
  - ICANN Universal Acceptance Steering Group (see https://community.icann.org/pages/viewpage.action?pageId=47255444)
  - fTLD has been effective in assisting in the resolution of some issues (e.g., Facebook, Verizon, Twitter); there is still much work to be done

- If you encounter an issue, please write to fTLD@fTLD.com with as much detail as possible

Resources

- Contact:
  - Craig Schwartz, fTLD, at fTLD@fTLD.com or 202.589.2532
  - Heather Diaz, fTLD, at fTLD@fTLD.com or 202.589.2404
  - Andrew Kennedy, BITS/FSR at Andrew.Kennedy@FSRoundtable.org or 202.589.2422

- Sign up to receive updates: www.ftld.com

- FAQ re: 2016 Security Requirements

- 2016 Security Requirements

- Redline of 2014 Security Requirements

Questions & Answers

Thank You