Email Authentication and Transport Layer Security (TLS)/Encryption
Implementation Guidelines

The following information is for Registrants of .BANK and .INSURANCE domain names (collectively an "fTLD Domain") to ensure compliance with the relevant requirements.

Email Authentication Requirement: Publish Domain-based Message Authentication, Reporting and Conformance (DMARC) record, plus Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) when domain is used for email.

Benefit: DMARC is a simple yet important security measure which prevents delivery of invalid or spoofed email purporting to originate from the fTLD Domain.

Implementation Guidelines
Registrants must publish a valid DMARC record under all circumstances, whether or not the fTLD Domain is used to send email. **For an fTLD Domain not used for sending email**: Registrants must publish a DMARC record with a reject mail receiver policy (p=reject). **For an fTLD Domain intended to send email**: Registrants must publish a DMARC record with a reject mail receiver policy (p=reject) unless in the implementation phase of email as described below. In addition, Registrants must also publish at least one of the following email authentication DNS Resource Records: • Sender Policy Framework (SPF), • DomainKeys Identified Mail (DKIM). It is recommended that DMARC records specify strict identifier alignment for both SPF and DKIM via the adkim and aspf tags. Also, for DMARC records published at an organizational domain level to set an appropriate sp: tag. When deploying DMARC during the implementation phase of email capabilities, Registrants may temporarily use a "none" (p=none) or "quarantine" (p=quarantine) mail receiver policy, but must change the policy to reject for ongoing operations within 90 days of deployment.

TLS/Encryption Requirements: Registrants must have a public key certificate (also known as a digital identity or TLS certificate) and TLS must be implemented using version 1.1 or greater where possible.

Benefit: Implementing TLS/Encryption is an important security measure protecting integrity and confidentiality of data and avoiding data tampering and eavesdropping, etc.

Implementation Guidelines

Registrants must use the encrypted version (HTTPS) of the domain for all electronic communications, including data in-transit, as detailed below. As .BANK and .INSURANCE are on the HSTS[1] preload list, domains that are not HTTPS compliant will not be accessible via browsers (like Chrome) following this list. As a global HSTS security policy becomes increasingly common, additional browsers are expected to block sites that are not HTTPS compliant.

An fTLD Domain is an HTTPS-only community. Registrants must have a public key certificate to secure their domains and sub-domains. Registrants may wish to use a wildcard certificate (e.g., *domainname.BANK) which allows a public key certificate to be used across single-level subdomains. Public key certificates must not be generated using any prohibited cipher suite components listed below.

TLS as follows applies to all domains and subdomains:

a. Web connections: TLS v1.1 or greater should be maintained. TLS v1.0 may be used to serve educational information about the importance of browser hygiene and provide guidance about how to update a browser.[2] Registrants should communicate to customers/visitors to their websites a specific date when access to their websites using TLS v1.0 will no longer be possible.

b. Server-to-Server Email: For domains sending or receiving email, TLS v1.1 or greater must be offered at the highest priority. However, when exchanging mail with a non-fTLD Domain earlier versions of TLS/SSL are permitted, including, as the lowest priority, defaulting to unencrypted email when it is not possible to provide encryption.

c. Other services: TLS v1.1 or greater should be used and TLS v1.0 does not need to be disabled at this time.

d. RFC 5746 must be implemented (prevents a known man-in-the-middle attack).

Prohibited Cipher Suite Components

The following is a non-exhaustive list of cipher suite components (authentication, encryption, message authentication code and key exchange algorithms) excluded from use with in-zone domains and in the generation of TLS certificates: Anon, CBC, DES, 3DES, FIPS, GOST 28147-89, IDEA, SEED, WITH_SEED, MD5, NULL, SHA (SHA1), RC4, EXPORT, EXPORT1024 and SRP.

[1] See HSTS information at https://www.ftld.com/december-5-2017/ and https://www.ftld.com/january-8-2018/
[2] For information on browser hygiene and security, please visit: https://www.ftld.com/secure-your-browser/