

REGISTRANT SECURITY REQUIREMENTS

REQUIREMENTS	✓ ACTION NEEDED	+ BENEFIT	👤 WHO CAN HELP
PRELIMINARY VERIFICATION	Verify: <ol style="list-style-type: none"> The domain name corresponds to your organization's legal name or brand; Your organization is eligible to apply for the domain name; The employee requesting the domain name on behalf of your organization is authorized to do so. 	Verification prevents cybersquatting and makes it impossible for bad actors to register a domain name or contact your customers while posing as your organization.	<ul style="list-style-type: none"> • fTLD • Approved registrars
1 ZONE	Ensure authoritative name server host names are within the .INSURANCE domain zone.	In-zone name servers place the same security requirements on the name server as the .INSURANCE domain itself.	<ul style="list-style-type: none"> • DNS provider • Approved registrars
2 ZONE	Implement Domain Name System Security Extensions (DNSSEC).	DNSSEC ensures that internet users are reaching your organization online and have not been redirected to a fraudulent website.	<ul style="list-style-type: none"> • DNS provider • Approved registrars
3 ENCRYPTION	Obtain a digital identity certificate.	Your .INSURANCE domain will resolve to HTTPS, which ensures all data is secure in transit.	<ul style="list-style-type: none"> • Certificate authority • Registrar • Web host
4 ENCRYPTION	Ensure Transport Layer Security (TLS) has been implemented using version 1.2 or greater where possible.	TLS creates an encrypted connection, protecting your website and visitors, securing email communications, and supporting the safe and secure transmission of information and transactions.	<ul style="list-style-type: none"> • Certificate authority • Registrar • Web host • Email provider
5 EMAIL AUTHENTICATION	Publish in DNS as a text record: <ol style="list-style-type: none"> Domain-based Message Authentication, Reporting, and Conformance (DMARC) record; Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) records when domain is used for email. 	DMARC helps protect against phishing and spoofing, and increases the deliverability of email to your customers, especially when used in combination with SPF and/or DKIM.	<ul style="list-style-type: none"> • Email security provider • Approved registrars