NIST SP 800-171 Revision 3 Self-Assessment

NIST 800-171

TROOTH, LLC NIST-800-171-2026-001

Document Title	NIST SP 800-171 Revision 3 Self-Assessment
Document ID	NIST-800-171-2026-001
Version	2.0
Classification	Public
Effective Date	September 18, 2026
Next Scheduled Review	March 18, 2027
Document Owner	D'Andre Heggie, Founder and Sole Member
Entity	Trooth, LLC
Supersedes	NIST SP 800-171 Revision 3 Self-Assessment Statement 1.0, June 8, 2026 (signed)
Reference Frameworks	NIST SP 800-171 Revision 3; NIST SP 800-171A Revision 3

1. Executive summary

This is Trooth, LLC's own self-assessment against NIST SP 800-171 Revision 3, carried out by the Founder using the assessment procedures of SP 800-171A. It is a self-assessment: no third party performed it, no third party reviewed it, and it is not a certification, a CMMC assessment or a submission to the Supplier Performance Risk System. It is published because buyers ask for it and because a self-assessment that names what is not met is worth more to them than a score. The Company processes no Controlled Unclassified Information on the effective date; this assessment states the posture a prospective federal-contract customer would inherit if it did.

2. Scope

Trooth, LLC (the Company) operates one product: the Trooth Network, a web application at trooth.co with a public API at api.trooth.co. A company connects its systems, the Network records what is true of them on a schedule with the source and the time of each observation, and buyers read that record. This statement covers that product, the production database that holds its data, the deployment pipeline that builds it, and the administrative accounts the Company holds with each provider named in its published Sub-processor List. It does not cover preview or development environments, which hold no customer data. As at the effective date the Company has no employees or contractors; every requirement written for personnel applies to the Founder today and to every future person from their first day.

3. Applicability

SP 800-171 protects Controlled Unclassified Information in nonfederal systems. Trooth, LLC holds no federal contract and processes no CUI on the effective date, so the publication does not apply to it as a matter of obligation. The Company assesses itself against it anyway, for two reasons: buyers who are themselves federal contractors ask whether a supplier could hold CUI safely, and the control families are a sound structure for a small company to check itself against. Where a requirement presumes an organisation with separate staff, facilities or classified network segments, this assessment says so rather than claiming a control that cannot exist here.

4. Assessment by family

Family	Position
3.1 Access Control	MET. Access is granted on a named need and removed on change; the runtime role holds the minimum privilege its purpose needs; tenant separation is enforced in the application from the session and again in the database by row-level security under a role that cannot bypass it, proven against a production-configured deployment by a live harness. Sessions are httpOnly, secure, same-site, with a fixed expiry. Remote access is over TLS only.
3.2 Awareness and Training	PARTIALLY MET. POL-16 requires security awareness training within thirty days of access and annually after. The Company has no employees; the Founder's first completion record does not yet exist, and the Trust Center states that control as not in place. Target: 31 October 2026.

Family	Position
3.3 Audit and Accountability	MET. Material actions are written to an append-only, hash-linked audit ledger; the chain is verified by a build gate and a break is an incident. Application errors, platform request logs, deploy history and provider audit logs are retained as ATT-01 sets out. No person, including the Founder, can alter a ledger entry through the application, and the runtime database role cannot either.
3.4 Configuration Management	MET. One path to production: a commit on the main branch that has passed one hundred and fifty-two gates. Dependencies install from a frozen lockfile and every third-party build action is pinned to a full commit hash. Inventories of routes, components and public files are generated from source and compared on every build, so configuration drift fails the deploy rather than accumulating.
3.5 Identification and Authentication	PARTIALLY MET. Multi-factor authentication is available to every account and required on every administrative account the Company holds with a provider. Passwords are stored as salted PBKDF2 hashes with a rising work factor. GAP: multi-factor recovery codes are not offered, which 3.5.3's intent would expect for continuity of access.
3.6 Incident Response	PARTIALLY MET. POL-09 sets four severities with response times from fifteen minutes, covers detection through post-mortem, and commits to customer notice within seventy-two hours where personal data is affected. GAP: the plan has not yet been exercised in a drill; the first is scheduled and the Trust Center states the control as not in place until the record exists.
3.7 Maintenance	MET, inherited. The Company operates no hardware and performs no physical maintenance. Platform maintenance is performed by the providers named in the Sub-processor List under their own published controls.
3.8 Media Protection	MET, by absence. The Company holds no removable media and no physical media of any kind. Backups are encrypted with AES-256 before they leave the runner that makes them and expire automatically on a thirty-day rolling window.
3.9 Personnel Security	NOT MET, and not yet applicable. The Company has no employees or contractors. Screening before production access and the offboarding sequence are written in POL-16 and apply to the first hire. The Trust Center states personnel screening as not in place.
3.10 Physical Protection	MET, inherited. The Company operates no facility. Its data rests in facilities run by Amazon Web Services, through Neon and Vercel, and by Cloudflare, each of which publishes independent audit reports for the physical and environmental controls of its sites. The Founder's workstation is full-disk encrypted with a screen lock and automatic updates, as POL-15 requires.

Family	Position
3.11 Risk Assessment	MET. A risk register records each identified risk with its likelihood, impact, the control that addresses it and the evidence for that control, and is re-read whenever the gate list or the published known-limitations record changes. Dependency and static analysis run on every push. GAP for 3.11.2(e): no independent penetration test has been performed; the Trust Center says so and the engagement is deferred until the first enterprise customer.
3.12 Security Assessment	PARTIALLY MET. Controls that a program can check are checked on every build and the deploy stops when one fails, which is a continuous assessment of most of this family. A plan of action exists for the eight controls the Trust Center names as not in place. No independent assessment has been performed.
3.13 System and Communications Protection	MET. TLS 1.2 or 1.3 on every connection with HSTS preloaded at a two-year max-age; AES-256 at rest in the managed database and its backups; a content security policy minted per request with a nonce and no inline script; one public port, 443; the database reachable only over TLS with credentials, from the application. Detail in ATT-03 and ATT-04.
3.14 System and Information Integrity	MET. Automated dependency advisories, static analysis and a secret scan on every push, with a second scan of the full history; error monitoring with personal data removed before an event leaves the server; external availability monitoring published on a public status page; and a post-deploy smoke that promotes the previous deployment back on failure.
3.15 Planning, 3.16 System and Services Acquisition, 3.17 Supply Chain Risk Management	PARTIALLY MET. Every sub-processor is engaged under a written data processing agreement, published with its purpose and region, and reviewed as POL-14 requires. Build inputs are pinned and workflows request read-only permissions except where a job must write. GAP: the software bill of materials served publicly describes the platform Workers rather than the web application; the Trust Center states that control as not in place.

5. Summary, stated honestly

Of the seventeen families, ten are met, six are partially met and one is not met and not yet applicable. The Company publishes no numeric score. A single number computed by the organisation assessing itself, against requirements it is not obliged to meet, for information it does not hold, would be a precise-looking figure with nothing behind it, and a buyer deserves the family-by-family position instead. The six partial answers trace to four underlying gaps, all of which the Trust Center already names as controls not in place: no training record yet, no incident-response drill yet, no independent penetration test, and no current software bill of materials for the web application. Three of the four have dates.

6. If Trooth were to process CUI

The Company would first put the four gaps above in place, complete a System Security Plan and a Plan of Action and Milestones in the form SP 800-171A expects, and agree the flow-down terms with the contracting customer before any CUI reached the Network. It would not accept CUI on the strength of this document. This statement describes a posture; it is not an offer to hold CUI and should not be read as one.

Reference: NIST SP 800-171 Revision 3; NIST SP 800-171A Revision 3. Related: POL-02; POL-03; POL-06; POL-07; POL-08; POL-09; POL-14; POL-15; POL-16; ATT-01; ATT-03; ATT-04; trooth.co/security.

Authorization

This statement is issued by Trooth, LLC under the authority of its Founder and Sole Member and describes the Company as it operates on its effective date. It is a published statement of the Company and requires no signature to bind it; the version published at trooth.co/security is the current one, and an earlier version, including any signed version of June 8, 2026, is superseded in full. It is not a certification and not an audit opinion: Trooth holds no audited certification against any framework and does not represent otherwise. Where this statement and the live service disagree, the service is corrected or the statement is re-issued, and the Company's published Trust Center states, control by control, what is in place and what is not.