CRITICAL INFRASTRUCTURE | CISA CYBERSECURITY PERFORMANCE GOALS 2.0

Token & CISA CPG 2.0

CISA released Cross-Sector Cybersecurity Performance Goals 2.0 (CPG 2.0) on December 11, 2025. CPG 2.0 is voluntary but anchors federal critical-infrastructure expectations and is now baseline language in most cyber insurance underwriting questionnaires. The goals are organized under the six NIST CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover. CPG 2.0 explicitly ranks hardware-based, phishing-resistant MFA (FIDO/WebAuthn or PKI) as the highest priority MFA option under Goal 2.H, ahead of mobile push, passkeys, and SMS. TokenCore Wearable and Token Portable are the FIDO2-certified, biometrically-verified, hardware-bound implementation that satisfies that ranking on day one.

Why Token Strengthens Your Security Posture

1. Highest priority MFA control by CISA's own ranking

CPG 2.0 Goal 2.H sequences MFA strength: hardware-based phishing-resistant first (FIDO / WebAuthn / PKI), then app-based soft tokens, then SMS / voice. Token is in tier one. Push MFA and OTP, what most peers run today, are explicitly second tier.

2. Defeats the threats CISA designed CPG to address

Origin-bound FIDO2 credentials and on-device biometrics defeat reverse-proxy, AiTM, push bombing, and helpdesk social engineering — the playbook behind Scattered Spider, Snowflake-customer compromise, and Change Healthcare. Hardware-bound credentials cannot be phished or replayed.

3. Documented evidence on day one

Every authentication produces a signed, attestable event, direct evidence for CPG self-attestation, regulator examinations, and insurer technical verification. CISO and Qualified Individuals can cite Token deployment as the documented control upgrade behind the annual program report.

CPG 2.0 – Token Mapping

§ CPG goal	What CPG 2.0 calls for	How Token addresses it
2.H · Phishing-Resistant MFA	Implement MFA across all IT accounts, prioritizing privileged administrative accounts. Hardware-based phishing-resistant MFA (FIDO/WebAuthn or PKI) is the highest priority option; OT environments must enable MFA on all remotely accessible accounts.	TokenCore Wearable and TokenCore Portable are FIDO2-certified, hardware-bound authenticators. Possession (the device) plus inherence (on-device fingerprint match) on every login. Match-on-chip biometrics: the fingerprint template never leaves the EAL5+ certified secure element. Tier one CPG 2.H control out of the box.
2.D · Revoke Credentials for Departing Employees	Document and immediately revoke access to information systems for departing employees and personnel.	Hardware-bound credential revocation is a single action in the IAM console, the credential dies with the device. No password rotation, no reset window, no help-desk social engineering vector. Direct evidence for the CPG 2.D self attestation.
1.A · Asset Inventory	Maintain a regularly updated inventory of all IT and OT assets, prioritizing those critical to business or operational functions.	Each Token authenticator is uniquely registered and inventoried; lost / found / replaced devices are managed through standard IAM lifecycle. Authenticator inventory feeds the broader CPG 1.A asset record on day one.
1.F · Third-Party Validation of Cybersecurity Control Effectiveness	Use third-party validation (independent assessments, penetration tests, etc.) to confirm cybersecurity controls are effective.	FIDO2 certification is independent third-party validation of authenticator design. Token is registered on the FIDO Alliance Certified Authenticator list and supplies the documented evidence regulators and insurers expect under 1.F.
Account Security Goals (Strong & Unique Credentials, Login Attempt Detection)	Eliminate weak / shared / reused credentials. Detect unsuccessful login attempts and respond to suspicious authentication patterns.	Token authenticators are passwordless. There are no shared, reused, or guessable credentials to compromise. Signed authentication events feed Splunk, Sentinel, Okta, and Microsoft Entra, provides the unsuccessful attempt and anomaly signal CPG calls for.
Vendor / Third-Party Access Goals	Apply the same access control standard to vendors, contractors, and remote maintenance accounts that touch IT or OT systems.	Same authenticator covers VPN, ZTNA, VDI, vendor jump hosts, and OT engineering workstations. Extends the CPG 2.H standard to MSPs, OEM service technicians, and remote OT vendors — supporting CPG 2.0's explicit OT remote access mandate.

CYBER INSURANCE | WHAT UNDERWRITERS WANT IN 2026

Phishing-resistant MFA is now a coverage and pricing lever, not a checkbox.

The cyber insurance market has shifted from questionnaire based assessment to technical underwriting: carriers verify the actual control, not the policy that describes it. CPG 2.0 Goal 2.H — hardware-based, phishing-resistant MFA — has become the baseline language carriers use to define adequate authentication. Customers running OTP, SMS, or push-only MFA are increasingly classified as below baseline risks: smaller limits, higher retentions, ransomware sub-limits, social engineering exclusions, or non-renewal at the next cycle.

MARKET POSTURE (2025–26)

~80%

of cyber insurers now require phishing-resistant MFA

Industry surveys of underwriting practice show phishing-resistant MFA has moved from "preferred" to "expected" across most major carriers. Beazley, Marsh-brokered placements, and standard market questionnaires now ask specifically whether MFA is phishing-resistant, not just present.

RANSOMWARE COVERAGE

Sub-limits

are commonly tied to MFA strength

Carriers routinely cap ransomware coverage (commonly 25–50% of the policy limit) for accounts that cannot evidence phishing-resistant MFA on privileged and remote access. Token deployment is the documented control change that supports requesting full-limit ransomware coverage at renewal.

SOCIAL ENGINEERING & FFT

Exclusion Risk

on accounts without hardware-bound MFA

Funds-transfer-fraud and social-engineering coverage is increasingly conditioned on phishing-resistant MFA for executives and finance roles. Hardware-bound authentication on the BEC blast radius — CFO, AP, payroll, treasury — is the underwriting signal that keeps these endorsements in scope.

PREMIUM & CAPACITY

Leverage

at renewal — capacity, retention, premium

Carriers reward documented control upgrades. Token deployment evidence (FIDO Certified ID, signed authentication logs, deployment scope) is exactly the technical attestation underwriters use to justify capacity expansion, retention reduction, or premium relief at renewal, even in a hardening market segment.

Token Products Referenced

TokenCore Wearable

FIDO2 authenticator. EAL5+ certified secure element, 508 DPI on-device fingerprint sensor, BLE + NFC. Match-on-chip biometrics; private keys never leave the ring. Designed for shared workstation retail, call center, and back office settings.

TokenCore Portable

Wireless FIDO2 hardware security key with on-device fingerprint sensor and secure element. Field-upgradable firmware. Drop-in replacement for OTP and tap-only keys for admin, developer, and TPSP workforce.