Touch to Trust – Hardware Rooted MFA for Nevada

Nevada Department of Taxation

State: Nevada
Submitting Agency: Nevada Department of Taxation
Award Category: Cybersecurity
Project Title: Touch-to-Trust – Hardware-Rooted MFA for Nevada Taxation
Project Dates: Pilot launch — September 2024 | 90 % adoption — January 2025 | 100 % enforcement — March 2025

James Underwood | Information Security Officer
Email: underwoodj@tax.state.nv.us | **Phone:** 775-430-0020

Executive Summary

Nevada Taxation processes more than **$9 billion** in yearly state revenue. This revenue helps support the State General Fund, education fund through the State Pupil's Centered Funding Plan, local government budgets, and the State Debt Service Fund. In 2024, the IRS issued interim guidance on authentication, stating that agencies should plan and begin to implement multifactor authentication for all system components. In addition, an internal survey revealed that approximately 2/3 of Taxation's staff regularly accesses the Internet as part of their job duties, creating a potential for malicious actors to take over systems by introducing malware through targeted or drive-by attacks. **Touch-to-Trust** set out to tackle these driving factors.

By pairing **YubiKey 5 NFC** tokens with an **active/active FortiAuthenticator 6.6.2** cluster in geographically split data centers, the project delivered strong MFA on every Windows system plus console access to firewalls, switches, and other sensitive systems. The roll-out progressed from a 25-user pilot in September 2024 to full enforcement in March 2025 without adding headcount.

Outcomes since enforcement day

- **100 %** MFA coverage for end user and privileged user accounts
- **0** lateral-movement incidents
- "Forgot my YubiKey" tickets average **≈ 2 per week** out of 425 users, each closed only after the original key is returned to spare inventory

IDEA – Why We Did It

- **Threat Vector:** 80 % of public-sector ransomware uses stolen or guessed credentials.
- **Compliance Imperative:** IRS Publication 1075 requires MFA for any system containing Federal Taxpayer Information.
- **Strategic Fit:** Advances OCIO's enterprise MFA roadmap and satisfies Nevada NRS 242's "reasonable security" standard.

Prompt	Response
What problem or opportunity does the project address?	Password-only logins left Nevada Taxation vulnerable to ransomware and IRS audit findings. Internal audit found 0 % MFA adoption; external guidance made MFA mandatory.
Why does it matter? (Business rationale)	A single compromised credential could halt revenue collection, disrupting ~$25 million/day in transfers to critical state programs. IRS non-compliance also jeopardized access to Federal Taxpayer Information.
What makes it different?	*Hardware-rooted* MFA (YubiKey touch) stops push-phishing fatigue and prevents remote attackers from completing logons—even if they have the password.
What makes it universal?	Aligns with State CIO Top Ten Priority #1 (Cybersecurity), IRS Pub 1075, CJIS Security Policy 5.6, and Nevada NRS 242 "reasonable security" language—pressures every state agency faces.

IMPLEMENTATION – How We Did It

Phase	Dates	Key Actions
Pilot (25 users)	Sep 2024	Pushed FortiAuthenticator client via GPOs 1–3; MFA optional.
Expansion (≈ 450 privileged & service accts)	October 2024 → Feb 2025	Hit 90 % adoption; weekend "tap & enroll" clinics; resolved Symantec false-positive.
Enforcement	Mar 2025	Applied GPO 4 **Fortinet MFA Mandatory**; blocked password-only logons.

Technical highlights

- **Token programming** – Slot 1 = standard user (short press), Slot 2 = system admin (long press).
- **RADIUS choice** – Time-based OTP (8-digit PIN appended to the password) used because FortiAuthenticator does not yet expose FIDO2 over RADIUS; legacy apps that insist on validating username/password locally forward only the OTP for second-factor approval.
- **Offline mode** – Each laptop allows **60** offline logins before it must reconnect to the Silvernet domain (office or VPN). The department initially set this number to **20** but increased it after some auditors in the field ran out during a work day. The system allows for up to **1000**.
- **Credential Providers** – All native Windows providers disabled; FortiAuthenticator provider and GINA client installed domain-wide.

IMPACT – What Changed

Metric	Pre-Project (FY 23)	Post-Project (FY 25)	Change
Non-privileged accounts protected by MFA	0 %	**100 %**	+100pts
Privileged accounts protected by MFA	0 %	**100 %**	+100pts
"Forgot YubiKey" replacement tickets	N/A	**≈ 2 per week**	–
Computer lateral-movement protection	Weak	**Strong**	Lower Risk

Historical password-reset data before December 2024 are unavailable due to a ticket-system migration; post-migration resets remain under five per month.

Cost & Resources

- **YubiKey 5 NFC:** 500 units × $50 ≈ **$25,000** (plus ≈ **$1000** for USB-C adapters, extension cables, quick-disconnect keyring kits)
- **FortiAuthenticator licenses:** ≈ **$7,500** (deployed on existing VM hosts)
- **Funding source:** MYNT (ARPA) cybersecurity allocation — no additional FTEs

Cost avoidance: Replacing a single ransomware recovery can top $1 million (NASCIO Cyber Disruption Study). Blocking lateral movement removes that tail-risk entirely.

Lessons Learned

- **Win over admins first** – Sysadmins were the toughest audience; demonstrating slot-2 "admin press" turned skeptics into champions.
- **Pre-clear AV signatures** – Symantec initially flagged a FortiAuthenticator DLL; submitting it as a false positive before mass deployment would have saved a day's scramble.
- **Stock spares** – A 5 % spare pool keeps operations smooth; true loss rate sits under 2 % thanks to quick-disconnect lanyards.

Why It's Worth the Investment

For <$35 k in hardware and licenses—and zero new staff—Nevada Taxation neutralized an enterprise-level cyber-risk, met federal audit requirements. That's a security return on investment any legislature can appreciate.

Conclusion

In less than six months, Nevada Taxation moved from "one stolen password away from catastrophe" to a hardware-rooted, tap-to-trust posture that blocks lateral movement cold and meets every federal audit line item. Nevada is building a safer digital frontier one YubiKey tap at a time.