Security Verification Toolkit

Executive Brief

Version 2.1.2 — February 2026

The Challenge

Federal compliance is expensive and slow.

- Manual security reviews take **weeks per project**
- Compliance gaps discovered late = **costly rework**
- ATO delays = **missed contract deadlines**
- No visibility into security posture **until audit time**

The Solution

Automated security scanning aligned to federal standards.

One command. Instant results. Audit-ready output.

```
./scripts/run-all-scans.sh /path/to/project
```

Bottom Line

¡ 5 min	35+	12	$0
Time to First Scan	Secret Patterns Detected	NIST Control Families	License Cost (MIT)

Why It Matters

Executive Concern	How We Address It
Cost Reduction	Replace 40+ hours of manual review with minutes of automated scanning
Risk Mitigation	Continuous detection of PII, secrets, and vulnerabilities before release
Compliance Speed	Pre-mapped to NIST 800-53 and 800-171 controls; PDF attestations ready for submittal
Audit Readiness	Checksummed, traceable evidence with file:line references

Scanning Capabilities

Category	What We Find
PII Detection	SSN, credit cards, phone numbers, emails, IP addresses
Secrets Detection	API keys, passwords, tokens, private keys (35+ patterns)
Malware Scanning	Malicious code detection via ClamAV integration
Vulnerability Assessment	CVE cross-reference via NVD and CISA KEV catalog
Host Security	OS configuration, encryption status, firewall settings

Federal Standards Coverage

Standard	Description	Status
NIST 800-53	Security and Privacy Controls	**12 control families**
NIST 800-171	Protecting CUI	**Mapped**
FIPS 199/200	Security Categorization	**Supported**

Platform Support

Platform	Status	Notes
macOS (Intel/ARM)	**Ready**	Full support
Linux (Ubuntu, CentOS, Debian)	**Ready**	Full support
Windows 10/11, Server 2016+	**Ready**	PowerShell + Git Bash
CI/CD Pipelines	**Ready**	GitHub Actions integrated
Air-Gapped Networks	**Ready**	Bundled threat intel

Recommended Next Steps

1. **Pilot** — Run on one project this week

2. **Evaluate** — Review findings and attestation quality

3. **Integrate** — Add to CI/CD pipeline

4. **Scale** — Roll out across project portfolio

Repository: github.com/brucedombrowski/security-toolkit

License: MIT (free, open source)

Questions: See SECURITY.md for contact information