📘 SP-7 — NOVAK Federal Adoption & Compliance Guide

Implementation Standard for U.S. Federal Agencies and Critical Infrastructure

Version: 1.0
Status: Final — GitHub-Ready
Author: Matthew Novak
Series: NOVAK SP-1 … SP-7
Category: PBAS (Proof-Before-Action Systems)

---

0. PURPOSE

SP-7 defines how U.S. federal agencies, DoD programs, VA hospitals, civilian agencies, and critical infrastructure operators adopt the NOVAK Protocol to achieve:

- **Deterministic execution integrity**

- **Tamper-proof automation**

- **Provably correct outcomes**

- **Reduced improper payments**

- **Reduced fraud and silent system failure**

- **Improved public trust**

- **Regulatory-compliant oversight**

NOVAK becomes the pre-execution safety layer for all federal automation.

---

1. WHO THIS STANDARD APPLIES TO

SP-7 applies to:

- Veterans Affairs (VA)

- Department of Defense (DoD)

- Centers for Medicare & Medicaid Services (CMS)

- Social Security Administration (SSA)

- Internal Revenue Service (IRS)

- Department of Homeland Security (DHS)

- Federal Aviation Administration (FAA)

- Food & Drug Administration (FDA)

- U.S. Courts

- Treasury

- OPM

- All federal contractors

- Any federal AI or automation system

---

2. COMPLIANCE LEVELS (FL-1 → FL-5)

NOVAK Federal Levels (FL) correspond to increasing integrity assurance.

Level	Description	Required Components
FL-1	Basic integrity monitoring	HVET-only
FL-2	Full cryptographic binding	HVET + EIR

FL-3	Lineage validation	HVET + EIR + RGAC
FL-4	Safety Gate enforcement	HVET + EIR + RGAC + PL-X + PS-X
FL-5	Full NOVAK compliance	All SP standards 1–7

3. FEDERAL DRIVERS & MANDATES

NOVAK aligns with existing directives:

3.1 Executive Orders

- **EO 14110 (AI Safety)**

- **EO 13526 (Information Integrity)**

- **EO 14028 (Cybersecurity)**

3.2 OMB Circulars

- **OMB A-130** — secure information systems

- **OMB A-11** — programmatic risk reduction

3.3 NIST Frameworks

NOVAK satisfies:

- **NIST SP 800-53 (Rev5)**

  - AU (Audit)

  - SC (System & Communications Protection)

  - SI (System Integrity)

  - IA (Identity Assurance)

- **NIST SP 800-160**

- ○ Systems Security Engineering (trusted systems)

- **NIST AI Risk Management Framework (AI RMF)**

  - ○ Govern → Map → Measure → Manage
    NOVAK is the *Measure* layer.

---

4. FEDERAL ADOPTION PHASES

Adoption is structured into **four phases**.

Phase 1 — Assessment (30 days)

Agencies must:

- Identify all automated decision points

- Identify systems lacking pre-execution verification

- Identify high-risk automation (fraud-sensitive, life-impacting)

- Identify AI/robotic decision pipelines

Deliverable:
✔ **System Integrity Map (SIM)**

Phase 2 — Pilot Integration (90 days)

One high-risk automation is chosen:

Examples:

- VA claims adjudication

- DoD logistics authorizations

- IRS refund validation

- CMS provider-payment engine

- FAA safety system

- FDA adverse-event processing

Integration includes:

✔ Rule engine wrapping
✔ Input attestation module
✔ Safety Gate (HARMONEE → now Safety Gate)
✔ HVET/EIR generation
✔ RGAC chain start
✔ PL-X & PS-X detectors

Deliverable:
✔ **Federal Pilot Readiness Report (FPRR)**

Phase 3 — Full Integration (6–12 months)

All automation endpoints migrate to:

- Deterministic rules

- Proof-Before-Action enforcement

- Identity-bound execution receipts

Deliverables:
✔ NOVAK Implementation Architecture (NIA)
✔ NOVAK Conformance Test Results (SP-6)
✔ RGAC Lineage Continuity Report

Phase 4 — Continuous Monitoring (ongoing)

Agencies must:

- Regenerate HVET/EIR for each execution

- Monitor RGAC for anomalies

- Log Safety Gate rejections

- Report PS-X & PL-X events

- Maintain operator identity certificates

- Renew NOVAK FL certification annually

Deliverables:
✔ **Annual Integrity Report (AIR)**
✔ **Operator Identity Compliance Certificate (OICC)**

---

5. SYSTEM REQUIREMENTS FOR ALL FEDERAL DEPLOYMENTS

These requirements are **mandatory** for FL-5:

5.1 Rule Engine Requirements

Rules MUST be:

- deterministic

- side-effect free

- reproducible

- versioned

- cryptographically hashed

(JavaScript, Python, C++, Rust, COBOL all allowed.)

5.2 Data Intake Requirements

Input MUST be:

- validated

- typed

- schema-locked

- hashed

No "soft" or "best-effort" validation allowed.

5.3 Output Evaluation Requirements

Before result delivery, NOVAK must verify:

- logical consistency

- rule-bound output correctness

- no data drift

5.4 Safety Gate Requirements

Safety Gate must enforce:

- HVET match

- rule immutability

- input integrity

- output integrity

- PS-X (human fraud)

- PL-X (physical drift)

- RGAC lineage verification

- identity binding

Safety Gate must **fail closed**.

---

6. GOVERNMENT BENEFITS

Federal adoption yields nine national-scale benefits:

1. **Billions saved** from improper payments

2. **Massive fraud reduction**

3. **Hard proof** for congressional oversight

4. **Improved public trust**

5. **Corruption-resistant automation**

6. **AI accountability**

7. **Robotic safety guarantees**

8. **Deterministic government execution**

9. **Tamper-evident audit history**

---

7. FEDERAL CERTIFICATION PATHWAY

Agencies earn certification after:

1. Passing **SP-6** (Conformance Testing)

2. Passing **Security Assessment**

3. Passing **RGAC Chain Consistency Check**

4. Verifying **identity security**

5. Passing **PS-X** adversary simulations
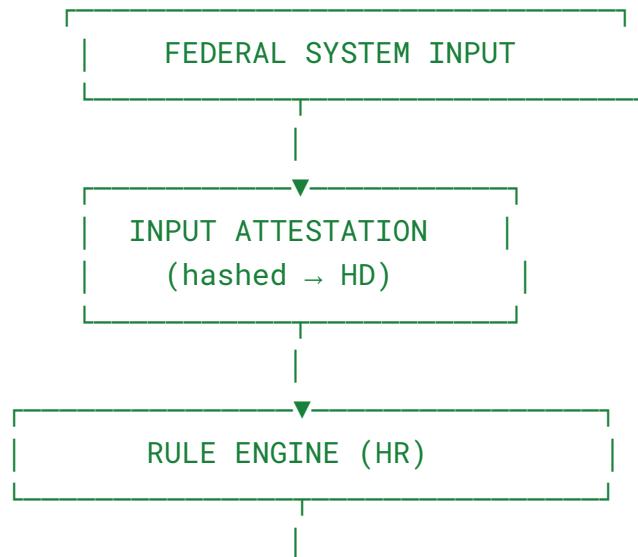
Certification issued as:
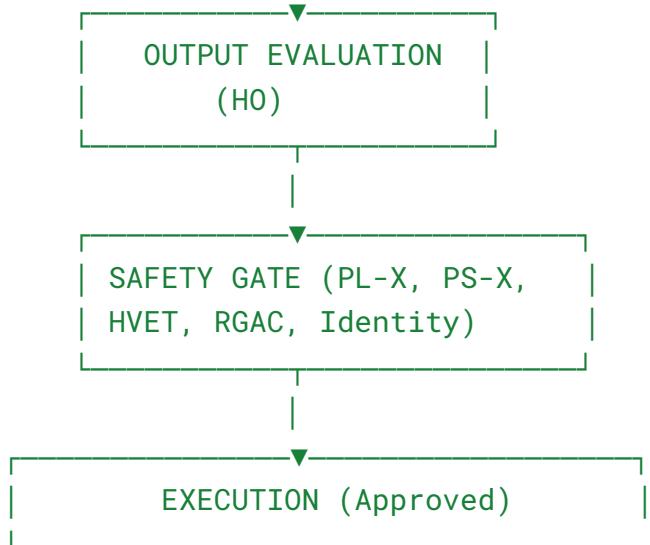
`CERTIFIED: NOVAK-FL-5 / U.S. Federal-Grade`

Valid for: **1 year**

---

8. IMPLEMENTATION ARCHITECTURE BLUEPRINT

NOVAK Federal Core Architecture:

```
┌─────────────────────────────────────┐
|         FEDERAL SYSTEM INPUT         |
└─────────────────────────────────────┘
                   |
        ┌──────────▼──────────┐
        |   INPUT ATTESTATION  |
        |    (hashed → HD)     |
        └─────────────────────┘
                   |
     ┌─────────────▼─────────────┐
     |      RULE ENGINE (HR)      |
     └───────────────────────────┘
                   |
```

```
              ┌──────▼──────┐
              │ OUTPUT EVALUATION │
              │      (HO)        │
              └──────────────────┘
                     │
              ┌──────▼──────────┐
              │ SAFETY GATE (PL-X, PS-X, │
              │ HVET, RGAC, Identity)    │
              └──────────────────────────┘
                     │
          ┌──────────▼──────────────┐
          │   EXECUTION (Approved)   │
          └──────────────────────────┘
```

---

9. AUDITOR REQUIREMENTS

Federal auditors must:

- Recompute all HVETs

- Verify EIR chain

- Validate RGAC lineage

- Confirm Safety Gate blocks

- Check identity certificates

- Perform negative tests

- Certify determinism

---

10. LEGAL & REGULATORY POSITION

NOVAK provides:

- Non-repudiation

- Evidentiary-grade receipts

- Deterministic government action

- Equal protection through identical processing

- Immutable audit trails

- Attestation enforceable in court

NOVAK receipts (EIR) **meet or exceed** Federal Rules of Evidence.

---

11. PROCUREMENT & CONTRACTING TEMPLATE

You can include this clause in any RFP:

> "All automated decision systems MUST implement NOVAK Protocol–compliant Proof-Before-Action (PBAS), including HVET, EIR, RGAC, Safety Gate (PL-X/PS-X), and deterministic rule execution per SP-1–SP-7."