VENIO

CHECKLIST 2026

FEDERAL & STATE AGENCY BUYER'S CHECKLIST

FedRAMP-Ready eDiscovery

What government teams must validate before any procurement discussion in 2026

73%

of agencies report FOIA backlog collisions with active litigation

$723M

government-wide FOIA processing cost in FY2024, up 22% YoY

12—18 mo

for traditional FedRAMP Moderate authorization

HOW TO USE THIS CHECKLIST

Walk each prospective eDiscovery vendor through these questions before any procurement discussion. Items marked MUST-HAVE are non-negotiable for federal compliance.

CRITICAL items require documented vendor answers before any RFP is issued. Items tagged STATE apply to state, local, and education (SLED) agencies governed by StateRAMP or state-specific records law.

All items tagged FEDERAL reference specific federal mandates.

LEGEND MUST-HAVE FEDERAL CRITICAL STATE

01

Authorization & Cloud Security Compliance

FedRAMP, StateRAMP, FISMA, CMMC - the non-negotiables before you open the RFP

FedRAMP / StateRAMP Status

- [ ] **1. Is your cloud offering authorized under FedRAMP, and at which impact level (Low / Moderate / High)?**

  MUST-HAVE · FEDERAL

  Federal agencies processing CUI or law enforcement data require at a minimum FedRAMP Moderate. DoD components must verify IL4/IL5 eligibility under DoD CC SRG. Ask for the package ID in the FedRAMP Marketplace.

- [ ] **2. What is the authorization date and the most recent Continuous Monitoring (ConMon) report status?**

  MUST-HAVE · FEDERAL

  FedRAMP authorization without active ConMon is a compliance gap. Confirm monthly POA&M updates are current, and no open High findings exist unresolved beyond 30 days.

- [ ] **3. For SLED agencies: Does your platform carry StateRAMP authorization (v2.0) or an equivalent state-accepted framework (TX-RAMP, IL-RAMP, NY Cyber)?**

  CRITICAL · STATE

  Several states now mandate StateRAMP authorization for cloud procurement. Confirm the authorization level and the states in which it is currently accepted.

- [ ] **4. Does the solution support on-premises or hybrid deployment for air-gapped or classified environments?**

  FEDERAL · CRITICAL

  Intelligence community components, law enforcement agencies, and classified DoD programs may be prohibited from using commercial cloud without an ATO. Ask whether the same core software runs on-prem with equivalent feature parity.

- [ ] **5. Is all government data stored exclusively in U.S.-based data centers with no cross-border data transfer?**

  MUST-HAVE · FEDERAL

  Required under OMB M-19-17 and applicable to all federal and most state agencies. Verify contractually and not just in the pitch deck.

Encryption, MFA & Zero Trust

- [ ] **1. Is data encrypted at rest (AES-256) and in transit (TLS 1.2+ minimum), and are encryption keys government-controlled?**

  Per NIST SP 800-111 and FIPS 140-2/3 requirements. Ask specifically whether agencies can manage their own KMS keys or whether the vendor holds sole custody.

  MUST-HAVE FEDERAL

- [ ] **2. Does the platform enforce phishing-resistant MFA (PIV/CAC or FIDO2) in a manner consistent with the OMB M-22-09 Zero Trust strategy?**

  SMS-based MFA no longer satisfies federal Zero Trust requirements. Confirm PIV/CAC integration is production-ready, not roadmap-only.

  MUST-HAVE FEDERAL

- [ ] **3. How does the vendor implement least-privilege access, role-based permissions, and attribute-based access controls (ABAC)?**

  Ask for a live demo of permission scoping, specifically, whether a FOIA analyst can be restricted from accessing litigation-only matters without manual workarounds.

  CRITICAL

⚠ **RED FLAG:**

Any vendor unable to produce a FedRAMP Package ID from the official marketplace (marketplace.fedramp.gov), or who claims "FedRAMP-ready" or "FedRAMP-equivalent" without an active ATO, should be immediately disqualified from federal procurement consideration. "In process" authorizations carry significant risk if your target go-live date is within 12 months.

02

FOIA & Public Records Compliance

5 U.S.C. § 552 · State FOIA statutes · OMB FOIA Guidelines 2023

☐ **1. Does the platform natively manage FOIA request intake, tracking, response generation, and statutory deadline enforcement within the same environment as litigation review?**

MUST-HAVE FEDERAL

Siloed FOIA tools create dual-track review problems. When FOIA and litigation touch the same document set, parallel workflows create inadvertent disclosure risk and audit failures.

☐ **2. Can the system enforce exemption application (b)(3), (b)(5), (b)(6), (b)(7)) with auditable, consistent tagging across reviewers?**

MUST-HAVE FEDERAL

Inconsistent exemption application is the leading cause of FOIA appeal losses and OIG referrals. Confirm that the system enforces exemption logic, not just labels.

☐ **3. For state agencies: Does the platform support your jurisdiction's specific public records statute (e.g., California PRA, Texas PIA, Florida Sunshine Law), including response deadlines and exemption mapping?**

CRITICAL STATE

State open records laws vary significantly in response timelines (5–10 business days vs. the federal 20-day standard), fee structures, and available exemptions. A federal-only FOIA workflow will generate compliance gaps at the state level.

☐ **4. Does the system generate defensible FOIA logs that satisfy DOJ OIP reporting requirements and can be exported for annual Chief FOIA Officer Report submissions?**

FEDERAL CRITICAL

OMB requires agencies to report on backlog, appeal rates, and processing times. Ask if this data flows automatically from the platform or requires manual compilation.

THE DUAL-TRACK DISCOVERY PROBLEM GOVERNMENT AGENCIES CAN'T IGNORE

Federal agencies are uniquely exposed to a scenario that private-sector legal teams rarely face: responding to a FOIA request and to active litigation involving the same underlying document set, simultaneously.

Without a unified platform, agencies routinely produce different versions of the same document across both tracks, creating Vaughn index errors, inadvertent waiver of privilege, and contradictory representations to different parties. A defensible eDiscovery platform must manage both tracks from a single, controlled data environment.

03 Records Management & Legal Hold

NARA GRS · Federal Records Act · State Records Retention Laws

- [ ] **1. Does the platform issue, track, and escalate legal holds with custodian-acknowledgment workflows, in a manner consistent with FRCP Rule 37(e) spoliation standards?** MUST-HAVE

  Litigation hold failures in government matters carry severe consequences, including adverse inference instructions and contempt sanctions. Custodian silence is not a hold. The system must enforce acknowledgment and auto-escalate non-responses.

- [ ] **2. Does the system integrate with NARA-approved records schedules (GRS 6.1, GRS 4.2) to prevent premature destruction of records subject to holds?** MUST-HAVE FEDERAL

  Agencies must demonstrate that litigation holds override scheduled disposition. A system that lacks native retention schedule integration creates conflicting destruction signals, a documented NARA compliance failure.

- [ ] **3. For state agencies: Does the system support state archives and records authority requirements, including state-mandated retention schedules and destruction certification?** CRITICAL STATE

  Most state records authorities require affirmative destruction certification upon disposition. Confirm the platform generates defensible destruction logs aligned with your state's specific authority.

- [ ] **4. Can the system collect from modern government data sources such as Microsoft 365 GCC/GCC High, SharePoint Online, Teams, Slack, legacy archives, and scanned paper records via OCR?** MUST-HAVE

  Agencies that migrated to M365 GCC or GCC High environments need connectors that are separately authorized for those tenants, standard commercial M365 connectors are not interchangeable. Confirm connector authorization levels.

04 Audit Defensibility & Chain of Custody

The standard that determines whether your discovery survives a challenge in court or OIG review

- [ ] **1. Does the platform produce an immutable, tamper-evident audit log of every user action, like search, review, tag, export, redaction, and hold modification?** — MUST-HAVE

  Government matters are uniquely exposed to congressional oversight, OIG investigations, and FOIA requests regarding the discovery process itself. Every action in your eDiscovery environment is a potential record. The log must be uneditable by anyone, including administrators.

- [ ] **2. Can the system produce a defensible chain-of-custody report for any document, showing every point of collection, processing, review, and production?** — MUST-HAVE

  Courts increasingly require government agencies to demonstrate the provenance of documents. Ask to see a sample chain-of-custody report, not a description of one.

- [ ] **3. Does the system support production in standard government formats (TIFF, native, load file, redacted PDF) and generate production logs that satisfy DOJ and court e-filing requirements?** — CRITICAL

  Productions missing required load file specifications (EDRM XML, DAT/OPT) or metadata fields have triggered sanctions in federal matters. Confirm format compliance with your litigation support team before signing.

- [ ] **4. Does the platform support privilege log generation, including AI-assisted privilege identification, in a format compliant with federal court local rules?** — FEDERAL, CRITICAL

  Privilege log production is one of the most resource-intensive steps in government litigation. Ask whether the platform can auto-draft privilege assertions based on document metadata and user-defined rules.

⚠ **RED FLAG:**

Any platform that allows administrators to edit or delete audit log entries, even for "error correction," fails the defensibility standard. Government counsel should treat audit log mutability as a disqualifying characteristic. Ask specifically: "Can your system administrators delete or modify audit log entries?" The correct answer is no, unconditionally.

05 AI-Assisted Review & Technology-Assisted Review (TAR)

Defensibility of AI outputs in government matters: the emerging litigation frontier

- [ ] **1. Can the vendor demonstrate the statistical validity and defensibility of its TAR/predictive coding workflow under the validated protocol standards of Maura R. Grossman and Gordon V. Cormack?**

  CRITICAL

  Courts in federal matters have increasingly scrutinized AI-assisted review methodology. Ask for a written methodology document, not a marketing one-pager that a testifying expert could defend.

- [ ] **2. Does the platform's AI operate on government data within the agency's authorized environment, without training on government data without explicit consent?**

  MUST-HAVE

  This is the AI data governance question that most agencies fail to ask. Government-sensitive data must never be used to train vendor models. Require this as an explicit contractual term, not just a verbal assurance.

- [ ] **3. Does the system support OCR with quality-control sampling for scanned paper records, a common gap in government legacy archive collections?**

  FEDERAL

  CRITICAL

  Federal agencies frequently hold decades of paper records in NARA-transferred archives. OCR accuracy below 95% on these collections has led to responsive document misses in significant government matters.

06

Procurement, Contract & Deployment

Vehicle access, deployment options, and total cost of ownership over the contract lifecycle

- [ ] **1. Is the solution available on a federal procurement vehicle (GSA MAS, SEWP V, CIO-SP4, NASA SEWP) to simplify acquisition?**

  MUST-HAVE · FEDERAL

  Sole-source justifications for eDiscovery software face increasing scrutiny. Confirm contract vehicle availability and whether pricing on the vehicle reflects actual deployment costs, not stripped-down base configurations.

- [ ] **2. For SLED agencies: Is the solution accessible through state cooperative purchasing agreements (NASPO ValuePoint, Sourcewell, state-specific TIPS)?**

  CRITICAL · STATE

  State procurement rules vary significantly. A vendor not available on your state's cooperative purchasing agreement may require a full competitive solicitation, adding 6-18 months to procurement timelines.

- [ ] **3. What are the total cost-of-ownership components? Specifically: data ingestion fees, per-GB storage costs, user licensing model, and overage charges during surge matters.**

  CRITICAL

  Government agencies often face sudden FOIA surges (congressional investigations, news cycles) that spike data volumes. An unpredictable pricing model will create exposure under the Antideficiency Act if costs exceed appropriated funds.

- [ ] **4. What is the vendor's data portability and exit policy? Can the agency retrieve all data and audit logs in non-proprietary formats upon contract termination?**

  MUST-HAVE

  Vendor lock-in in eDiscovery is particularly damaging for ongoing government matters that span contract terms. Require contractual guarantees of EDRM-standard data export at any time, without fee.

- [ ] **5. Does the vendor offer a proof-of-concept (POC) period using real agency workflows rather than sanitized demo data before full commitment?**

  CRITICAL

  A vendor confident in their platform will support a 30-90 day POC against your actual FOIA and litigation workflows. Resistance to real-data POC is a significant evaluation signal.

07 Implementation, Training & SLA

The implementation gap is where most government eDiscovery projects fail, before the first document is reviewed.

- [ ] **1. Does the vendor have demonstrated experience with government implementations, specifically FISMA-compliant onboarding, government network constraints, and CAC/PIV integration in production environments?** MUST-HAVE

  Ask for references from comparable federal or state agencies, not enterprise commercial clients. Government network environments (DISA STIG compliance, GFE restrictions, proxy configurations) create implementation challenges that commercial clients never encounter.

- [ ] **2. What SLAs does the vendor provide for uptime, incident response, and support escalation, and are penalties for SLA breach contractually enforceable?** CRITICAL

  Court-ordered production deadlines don't accommodate vendor outages. Confirm that uptime SLAs (minimum 99.9%) are contractually guaranteed with liquidated damages, not just aspirational targets.

- [ ] **3. Is ongoing training, system administration support, and surge staffing included, or separately scoped and priced?** CRITICAL

  Government agencies frequently experience personnel turnover that resets institutional knowledge of complex platforms. Confirm whether training is unlimited and included, or whether it triggers additional contract modifications.

Before You Issue the RFP: The Three Questions That Separate Defensible Platforms from Risky Ones

1. **"Show me your FedRAMP Package ID in the marketplace, right now."**

   Any hesitation or redirect is your answer.

2. **"Can your administrators delete or modify audit log entries?"**

   The only acceptable answer is an unconditional no.

3. **"Will you run a 60-day POC against our actual FOIA and litigation workflows before we commit?"**

   A confident platform vendor will say yes. A vendor who won't let you test against real workflows isn't confident in their product.

Purpose-built eDiscovery for government legal, records, and compliance teams. Trusted by federal civilian agencies, defense components, and state governments managing FOIA, litigation, and audit discovery at scale.

FedRAMP-authorized · FISMA-ready · Hybrid deployment supported

See Government eDiscovery Solutions

Ready to walk through this checklist with a vendor who can answer every question?

Request a 30-minute discovery call, and we'll run through your agency's specific FOIA, litigation, and audit workflows, no boilerplate demo required.

See Venio eDiscovery in action

Book a 30-Minute Live Demo

VENIO


Venio
Review
Venio
Legal Hold
Venio ECA
AI
Venio
AI Review
Venio
Production