

ADDENDUM D: THE EXPLAINABILITY & RED FLAG MANDATE

Purpose: To eliminate the "Technical Ignorance" defense and establish a strict standard of accountability for officials overseeing automated systems.

I. MANDATORY EXPLAINABILITY CERTIFICATION

Every federal budget, appropriation request, or performance report involving data generated by automated systems (including AI, robotics, or precision sensors) must include a **Signed Explainability Certification**.

- The official must swear that they have reviewed the data's logic and "provenance" (origin).
- Lack of technical expertise shall not be a valid defense for signing a fraudulent certification. If an official does not understand the data, they are legally prohibited from certifying it.

II. LEGAL PRESUMPTION OF KNOWLEDGE (RED FLAGS)

- **Presumed Liability:** If an automated system generates an "Error Code," "Discrepancy Alert," or "Red Flag" notification, the certifying official is **legally deemed to have actual knowledge** of that alert.
- **The "Notification is Knowledge" Rule:** Proof that a "Red Flag" was delivered to the official's digital dashboard or agency server is sufficient to satisfy the "Knowledge" requirement for Official Fraud.

III. THE IGNORANCE EXCLUSION (ANTI-LOOPHOLE)

- **No Technical Immunity:** Claiming a lack of technical understanding regarding a system-generated "Red Flag" does not negate "Reckless Disregard."
- **The "Owner" Principle:** By signing the document, the official assumes full personal liability for the truth of the data. Ignorance of how a system failed is legally equivalent to knowing it failed and hiding it.