

10-minute presentation: Put enforceable safeguards around terrorist watchlisting

Open with the request

- Thank you for meeting with me. I am asking your office to sponsor the Terrorist Screening Integrity and Due Process Act of 2026 and support rigorous oversight of how Americans are placed on terrorist watchlists and how their information is used.
- A law-abiding person should have a meaningful way to challenge a terrorism designation, correct a mistaken identity, and stop unauthorized use of the record. The government should have to justify that designation before an independent judge. These protections should apply under every administration.

Explain the categories precisely

- The Justice Department Inspector General's 2005 audit publicly identified Handling Codes 3 and 4 as the two lowest levels of law-enforcement response, while redacting their detailed definitions. The report explained that Code 4 could include associates of suspected terrorists who might not themselves pose a direct terrorist threat. These are historical handling codes; Congress should require disclosure of their current equivalents and governing rules.
- The distinction matters: being associated with someone is not the same as personally preparing an act of terrorism. A label that affects a citizen's treatment should rest on reliable, individualized evidence. The bill makes that principle enforceable.
- Under sections 5 and 11, U.S. persons could not remain listed solely in those legacy or equivalent categories. The government would have to satisfy the bill's specific No Fly or Selectee standards, identity requirements, and judicial process. Renaming a category would not excuse an unsupported record.

Show why internal assurances are insufficient

- The 2007 Inspector General follow-up found that 38 percent of 105 records tested after routine quality review still contained errors or inconsistencies. It also reported that 45 percent of watchlist records referred for redress review after positive-match encounters required modification or removal. Those are findings about the reviewed records, not estimates of today's entire watchlist. They demonstrate why independent review and enforceable correction duties matter.
- In 2023, the Senate Homeland Security Committee's majority-staff report identified opaque redress and fragmented oversight. It reported that more than 500 private-sector entities had access to a subset of watchlist information for law-enforcement purposes, including police or security forces at colleges, hospitals, and prisons.
- An error can therefore matter beyond the office that created it. Congress should require every authorized recipient to document its use, correct mistakes, and stop circulating deleted records. A correction that never reaches the next screening system leaves the affected person carrying the burden.

Request an investigation of alleged misuse

- I also ask your office to investigate allegations of government weaponization and nonconsensual human experimentation, including the claim that watchlist information has been used as a roster to select or track people for those purposes. The cited watchlist audits do not establish that claim. Congress should evaluate specific evidence and require accountable answers through the appropriate oversight channels.
- The Senate's 1977 MKULTRA hearing documented covert testing involving unwitting people. That historical record demonstrates the importance of independent oversight; it does not, by itself, establish a present-day connection to terrorist watchlisting.
- Please request preservation and independent examination of relevant nomination records, access logs, disclosures, complaints, and supporting documents. Where evidence identifies a relevant program or contractor, seek its authorizations, contracts, and human-subject protections through the committees entitled to review them. Protect complainants and witnesses against retaliation, and report substantiated findings and corrective action.

Explain what the bill would change

- Require proof and independent review. Sections 4 through 8 require corroborated facts and probable cause tied to terrorism-related conduct, with defined No Fly and Selectee criteria. Protected speech, religion, peaceful protest, family relationships, and uncorroborated accusations cannot substitute for evidence. A designated judicial panel and independent, security-cleared advocates would test the government's case.
- Correct identities and remove unsupported records. Sections 5, 9, 11, and 12 require minimum identifiers, special protections for children, initial removal of specified deficient legacy records within 30 days, and judicial review of remaining legacy records within 180 days, subject to narrow judicial holds. Automatic removal duties and notices to downstream recipients address stale and mistaken records.
- Restrict use and prevent evasion. Sections 5 and 13 limit permitted uses, require access logs and recipient accountability, and prohibit substitute watchlists used to evade the Act. A terrorism designation should not become a general-purpose tool for punishing a person or restricting ordinary civic and economic life.
- Give people an enforceable remedy. Section 10 provides a single redress portal, response deadlines, identity correction, judicial relief, attorney's fees, and damages for qualifying knowing or willful violations. It expressly protects against retaliation for protected activity or seeking redress.
- Preserve the ability to address genuine threats. Section 8 permits a 72-hour emergency judicial order and one extension of up to seven days on a renewed showing. Sections 15 through 17 add audits, reporting, funding, and accountability. The government retains a preventive tool, with rules that can be enforced.

Close with a concrete commitment

- This is a practical opportunity to protect national security and constitutional rights together. Accurate records help officials focus on genuine threats. Judicial review protects people from unsupported designations. Enforceable limits on sharing and use make abuse easier to detect and stop.
- Will your office designate a legislative staff member to review this draft for sponsorship, request a committee briefing on watchlist categories and downstream access, and pursue the evidence-preservation and oversight requests I have described?
- May we agree on a staff contact and a follow-up date within two weeks? I will provide the draft, the primary-source reports, and any specific supporting records available for the office's review. A promise of fair treatment becomes meaningful when a person can enforce it.

Quick answers and source notes (Reference page for preparation and follow-up; not part of the presentation).

Does the record prove an experimentation roster? The cited audits establish watchlist-management problems, not that allegation. Ask the office to evaluate specific documents and testimony through an independent inquiry. A screening delay alone does not establish watchlist placement or experimentation.

Are Handling Codes 3 and 4 two current secret lists? Use the precise historical terminology. The 2005 audit publicly identified the codes but redacted their detailed definitions. Ask for current categories and successor rules; do not assume the historical structure is unchanged.

Why probable cause if this is preventive? The draft reaches corroborated concrete operational steps toward terrorism-related conduct. It does not require a completed offense. Describe probable cause as the protection this bill would enact, not as a universal statement of current constitutional law.

Does the bill already mandate an experimentation inquiry? No. The current draft regulates watchlisting and its uses. The focused inquiry described here is a separate oversight request; any express human-experimentation provision would require additional legislative text.