

DISCUSSION DRAFT

119TH CONGRESS

2D SESSION

H. R. ____

TERRORIST SCREENING INTEGRITY AND DUE PROCESS ACT OF 2026

A BILL

To codify standards governing the inclusion of United States persons in the federal terrorist watchlist; improve the accuracy, integrity, and national-security value of terrorist screening; provide meaningful notice, review, and redress; prohibit unauthorized shadow watchlists based on constitutionally protected activity; and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

September __, 2026

Mr./Ms. _____ introduced the following bill; which was referred to the Committee on _____

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

BIPARTISAN PURPOSE OF THE DISCUSSION DRAFT

This proposal is designed around a principle that should command support across party lines: a terrorist watchlist must be accurate enough to identify genuine threats, disciplined enough not to divert scarce counterterrorism resources toward erroneous records, and constrained enough to protect the constitutional rights of United States citizens and lawful permanent residents. The same quality-control defects that can burden innocent people can also cause true threats to be missed. The bill therefore treats national security and civil liberty as mutually reinforcing objectives.

The federal consolidated terrorist watchlist was created after September 11, 2001, under Homeland Security Presidential Directive 6, which itself required implementation consistent with the Constitution and laws protecting Americans.[1] The Terrorist Screening Center was renamed the Threat Screening Center in March 2025 as its mission expanded.[2] Twenty-five years after the attacks, Congress has a responsibility to place durable statutory limits, transparent oversight, and enforceable procedures around the treatment of United States persons in this powerful screening architecture.

This draft deliberately does not depend on confidence in any particular President, Attorney General, FBI Director, political party, or administration. It builds rules that apply regardless of who controls the Executive Branch.

The draft also separates verified oversight findings from claims that are not established by the public record. A source-verification memorandum following the bill identifies several such distinctions so that congressional sponsors can defend every factual assertion in the legislative record.

SECTION 1. SHORT TITLE.

This Act may be cited as the “Terrorist Screening Integrity and Due Process Act of 2026”.

SEC. 2. CONGRESSIONAL FINDINGS.

- (1) On September 16, 2003, Homeland Security Presidential Directive 6 (“HSPD-6”) directed the Attorney General to establish an organization to consolidate the Federal Government’s approach to terrorism screening and required safeguards for information concerning United States persons. HSPD-6 further required that the directive be implemented consistently with the Constitution and applicable law.[3]
- (2) The resulting consolidated terrorist watchlist was developed principally through executive directives, interagency memoranda, classified or controlled watchlisting guidance, agency policy, and screening authorities enacted for particular purposes. Congress has not enacted a comprehensive statute establishing the substantive standard, nomination route, retention standard, notice rule, and redress rights governing inclusion of United States persons in the core terrorist screening dataset.

- (3) The Department of Justice Office of the Inspector General (“DOJ OIG”) has repeatedly identified weaknesses in terrorist watchlisting data quality, nomination controls, modification and removal practices, handling instructions, duplication, recordkeeping, and redress.
- (4) In 2005, the DOJ OIG examined a subset of 109,849 watchlist records and reported that 22.04 percent were assigned Handling Code 3 and 74.64 percent were assigned Handling Code 4, for a combined 96.68 percent in the two lowest handling categories. The OIG explained that Handling Code 4 records could include associates who might not pose a direct terrorist threat and frequently lacked sufficient identifying information for a higher handling code.[4]
- (5) The 2005 audit also identified records with handling codes inconsistent with other information in the records, tens of thousands of records containing an “armed and dangerous” indicator paired with the lowest response instruction, and hundreds of records lacking a handling code, demonstrating the operational consequences of data-integrity defects.[5]
- (6) In 2007, the DOJ OIG found that the Terrorist Screening Center continued operating two versions of the consolidated database without adequate assurance that their contents were identical, identified significant duplicate records, and found that internal FBI processes could bypass the normal nomination flow.[6]
- (7) The 2007 follow-up audit found that 38 percent of 105 records that had undergone routine quality-assurance review still contained errors or inconsistencies not identified by the Center’s review; it further reported that 45 percent of watchlist records referred for redress review after positive-match encounters required modification or removal.[7]
- (8) In 2008, the DOJ OIG reported that FBI field-office submissions were often incomplete or inaccurate, that field offices had at times bypassed FBI Headquarters and submitted nominations directly to the National Counterterrorism Center (“NCTC”), and that this could result in watchlisting without an FBI quality review. [8]
- (9) The same 2008 audit found that policies governing non-investigative-subject nominations lacked procedures for modification or removal and lacked quality-control mechanisms; the OIG learned that NCTC was receiving some non-investigative-subject nominations directly from FBI field personnel, with no mechanism to ensure that such nominations were appropriate, complete, accurate, updated, or removed when necessary. [9]
- (10) In 2009, the DOJ OIG found that the FBI failed to nominate subjects in 15 percent of sampled terrorism investigations, processed 78 percent of reviewed initial nominations outside established timeframes, failed to submit required modifications in 67 percent of cases in which modification was necessary, failed to remove subjects as required in 8 percent of reviewed closed cases, and failed to remove subjects timely in 72 percent of reviewed closed cases.[10] These deficiencies threatened both security and accuracy.
- (11) The 2009 audit further found that internal controls over several non-standard processes for nominating non-investigative subjects were weak or nonexistent; more than 62,000 nominations had been made through non-standard FBI processes, and the OIG found almost 24,000 FBI watchlist records not sourced to a current terrorism case classification, including records based on cases closed years earlier that should have been removed and that caused unnecessary screening.[11]
- (12) In 2014, the DOJ OIG again reported that FBI time requirements for watchlist actions could be strengthened and that the database used to submit, monitor, and track non-investigative-subject nominations had weaknesses, notwithstanding improvements made after earlier audits.[12]
- (13) In December 2023, majority staff of the Senate Committee on Homeland Security and Governmental Affairs, under Chairman Gary Peters, issued “Misleading as a Threat,” finding a layered and duplicative screening system, at least 22 mechanisms that can lead to additional screening or denial of travel, approximately 1.8 million terrorist-watchlist records as of November 2022 compared with approximately 150,000 in 2004, and an opaque redress structure that can leave Americans without actionable information. [13]
- (14) The Peters report stated that the executive branch had revealed little information about what watchlists it maintains, who is included, why and how the lists are used, or which agencies and private-sector entities have access; the report found that more than 500 private-sector entities had access to a subset of watchlist information for law-enforcement purposes.[14]
- (15) The Peters report concluded that the government was not holistically assessing the combined effects of its screening architecture, that the redress process was not transparent, and that oversight had been fragmented,

preventing a comprehensive and consistent independent assessment. The report recommended a coordinated full-scope Inspector General review, meaningful redress, annual reporting, and congressional evaluation of constitutional protections.[15]

- (16) The Peters report recognized concerns with the “reasonable suspicion” threshold, while also acknowledging appellate precedent holding that reasonable suspicion can satisfy due process in this context. Congress possesses authority to enact a higher statutory protection for United States persons than the constitutional floor identified by those courts.[16]
- (17) A 2014 district-court decision held that the then-existing DHS Traveler Redress Inquiry Program was “wholly ineffective” and lacked meaningful procedures for U.S. citizens challenging placement on the No Fly List, prompting revised procedures that now provide U.S. persons on the No Fly List some notice and opportunity to challenge their placement.[17] Meaningful safeguards should not turn solely on whether a person is denied boarding.
- (18) The public record contains documented instances of innocent individuals being misidentified or erroneously placed on aviation watchlists, including a case in which a traveler was mistakenly placed on the No Fly List because an FBI agent misread a form.[18]
- (19) Current FBI public guidance states that only government agencies may nominate an individual to the federal terrorism watchlist and that protected First Amendment activity, race, ethnicity, religion, guesses, or hunches may not by themselves be the basis for inclusion.[19] Congress should codify these limitations, require corroboration of private-source allegations, and make them judicially enforceable.
- (20) In 2026, a recorded statement attributed to an ICE officer about placing a peaceful observer in a “nice little database” labeling her a domestic terrorist prompted formal congressional oversight. A Senate letter treated the alleged database as a grave constitutional concern; ICE subsequently denied maintaining a database of United States citizens merely for protesting while acknowledging certain information collection for law-enforcement and officer-safety purposes.[20] Regardless of the factual dispute concerning that episode, Federal law should prohibit any shadow watchlist based on protected speech, protest, petition, association, journalism, or observation of government activity.
- (21) The Department of Defense publicly identifies a Machine-assisted Analytic Rapid-repository System (“MARS”) as an intelligence/data capability.[21] The public record reviewed for this draft does not establish that MARS is a replica of the TSDS. Congress should nevertheless prohibit any agency from using MARS or any other system to evade the substantive and procedural safeguards applicable to United States-person terrorist watchlisting.
- (22) On the twenty-fifth anniversary of the September 11, 2001 attacks, Congress should preserve the capacity to identify genuine terrorist threats while ensuring that an extraordinary post-9/11 screening architecture operates under clear law, meaningful judicial review, accurate records, individualized evidence, and enforceable constitutional safeguards.
- (23) Accuracy is a national-security requirement. A record that wrongly burdens an innocent person consumes screening and investigative resources that should be focused on actual threats; a record that fails to include or update accurate information can allow a genuine threat to evade detection.
- (24) No administration should possess unchecked power to impose secret, potentially long-lasting government consequences on a United States person based on an unreviewed accusation, stale record, mistake, guilt by association, or constitutionally protected activity.

SEC. 3. PURPOSES.

- (1) to provide a comprehensive statutory framework governing terrorist watchlisting of United States persons;
- (2) to raise the evidentiary threshold for placement of a United States person on the terrorist watchlist from reasonable suspicion to probable cause as a matter of Federal statutory law;
- (3) to ensure centralized quality control and prohibit direct field-office nominations to the TSDS;
- (4) to require notice and a meaningful opportunity to contest a proposed or emergency listing, subject to narrowly tailored national-security procedures approved by an Article III judge;
- (5) to provide every United States person a workable mechanism to learn whether the person is listed, obtain a meaningful statement of reasons, and seek correction or removal under this Act and the Privacy Act of 1974;

- (6) to require staged review and prompt removal of legacy United States-person records that cannot satisfy the new probable-cause and identity-quality standards;
- (7) to prohibit duplicative, derivative, informal, or “shadow” terrorist watchlists that evade this Act; and
- (8) to protect national security by ensuring that watchlisting resources are concentrated on persons for whom reliable evidence supports a genuine terrorism-related threat.

SEC. 4. DEFINITIONS.

In this Act:

- (1) **APPROPRIATE COURT.**—The term “appropriate court” means the United States Terrorist Screening Review Panel established under section 7.
- (2) **CONCRETE OPERATIONAL STEP.**—The term means an objectively verifiable act that materially advances the planning, preparation, direction, financing, procurement, concealment, or execution of terrorism or knowing material support, and does not include protected activity, status, belief, association, or presence alone.
- (3) **DERIVATIVE WATCHLIST.**—The term means any database, dataset, index, file, application, model, score, alert, record system, or designation that imports, mirrors, reproduces, infers, or operationalizes the terrorist-watchlist status of a United States person.
- (4) **MINIMUM IDENTIFIERS.**—The term means the person’s full legal name, date of birth, and at least one unique identifier consisting of a passport number, Social Security number or Individual Taxpayer Identification Number, alien registration number, or biometric identifier verified as belonging to that person.
- (5) **NO FLY CATEGORY.**—The term means the category authorized only when probable cause establishes that a person is preparing, directing, committing, or knowingly materially supporting an act of terrorism involving civil aviation or mass-casualty violence, and the court finds by clear and convincing evidence that enhanced screening or another less restrictive measure would be inadequate to address the identified risk.
- (6) **PROBABLE CAUSE.**—The term means reliable and sufficiently corroborated facts and circumstances that would warrant a person of reasonable caution to believe that the United States person—
 - (A) knowingly has engaged in, is engaging in, or is preparing to engage in conduct constituting international terrorism or domestic terrorism under section 2331 of title 18, United States Code, an offense under section 2332b of that title, or conduct constituting knowing material support under section 2339A or 2339B of that title; or
 - (B) is taking concrete operational steps toward such conduct. Mere association, familial or household relationship, ideology, religion, race, ethnicity, speech, protest, petition, journalism, legal representation, litigation, travel pattern without corroborating conduct, anonymous accusation, uncorroborated tip, or intelligence hunch does not, alone or in combination with other protected activity, establish probable cause.
- (7) **PROTECTED ACTIVITY.**—The term means conduct protected by the Constitution or Federal law, including speech, press activity, petitioning, religious exercise, peaceful assembly, peaceful protest, political advocacy, association, journalism, legal representation, litigation, protected whistleblowing, and lawfully recording or observing government officers.
- (8) **SELECTEE CATEGORY.**—The term means the category authorized only when probable cause establishes terrorism-related conduct under paragraph (6), but the court finds that the residual risk can be adequately managed by enhanced aviation screening rather than denial of boarding.
- (9) **TERRORIST SCREENING DATASET OR TSDS.**—The term means the consolidated Federal terrorist watchlist historically known as the Terrorist Screening Database or TSDB, together with successor systems or datasets maintained by or for the Threat Screening Center.
- (10) **THREAT SCREENING CENTER.**—The term means the FBI-administered entity formerly known as the Terrorist Screening Center, or any successor entity.
- (11) **UNITED STATES PERSON.**—The term means a United States citizen or national or an alien lawfully admitted for permanent residence, including a dual national. A person who becomes a United States person after being listed shall receive the protections of this Act immediately upon the Government’s actual or constructive notice of that status.

SEC. 5. STATUTORY AUTHORIZATION; CATEGORIES; IDENTITY QUALITY; LIMITS ON USE.

(a) AUTHORIZATION.—The Attorney General, acting through the Federal Bureau of Investigation and the Threat Screening Center, may maintain the TSDS subject to this Act.

(b) EXCLUSIVE CATEGORIES.—A United States person may be included in the TSDS only in the No Fly category or Selectee category, and only pursuant to section 7 or 8. No United States person may be maintained solely in a general encounter, intelligence-collection, expanded-selectee, legacy Handling Code 3 or 4, or functionally equivalent category.

(c) CATEGORY-SPECIFIC FINDINGS.—Every order shall identify the authorized category and make the findings required by section 4(5) or 4(8). The Government may not seek No Fly status when Selectee measures would adequately manage the proven risk.

(d) INDIVIDUALIZED BASIS.—No person may be listed merely because the person is a relative, household member, associate, coworker, client, attorney, business partner, social-media contact, political associate, or member of the same organization as another listed or suspected person.

(e) MINIMUM IDENTIFIER RULE.—No United States-person record may be entered, retained, disseminated, or matched as TSDS status unless it contains the minimum identifiers. A name-only or name-and-date-of-birth-only record is prohibited.

(f) POSSIBLE-MATCH FLAG.—An agency may maintain a temporary possible-match flag for identity resolution if the flag—

- (1) is conspicuously designated as not constituting terrorist-watchlist status;
- (2) may cause only a single, minimally intrusive identity-verification inquiry and may not cause denial of boarding, repeated secondary screening, arrest, detention, or dissemination as a terrorist match;
- (3) is resolved or deleted within 72 hours; and
- (4) is recorded in an auditable log.

(g) **PURPOSE LIMITATION.**—TSDS-derived information concerning a United States person may be used only for aviation screening authorized by this Act or a documented officer-safety inquiry during a lawful encounter. It may not be used for employment, banking, lending, licensing, housing, insurance, education, public benefits, commercial scoring, or another civil determination unless a separate Act of Congress expressly authorizes that use and provides due process.

(h) **RECIPIENT CONTROLS.**—Every recipient shall execute a written purpose-limitation agreement, maintain query and dissemination logs, recertify access annually, and comply with machine-readable correction and deletion notices. Access shall be suspended immediately upon failure to certify deletion or material noncompliance.

SEC. 6. EXCLUSIVE NOMINATION CHANNEL AND SOURCE RELIABILITY.

(a) **NO DIRECT FIELD SUBMISSION.**—No field office, Joint Terrorism Task Force, Legal Attaché office, fusion center, or individual employee may submit a United States-person nomination directly to the Threat Screening Center, NCTC watchlisting personnel, a downstream screening database, or any repository capable of generating TSDS status.

(b) **HEADQUARTERS REVIEW.**—A field-originated proposal shall first be reviewed by headquarters counsel and a Senate-confirmed officer or properly delegated senior official, who shall certify that probable cause and the proposed category criteria are met; minimum identifiers are verified; all material exculpatory and source-reliability information is included; and the proposal is not based on protected activity, retaliation, refusal to serve as an informant, personal animus, a private dispute, or an uncorroborated allegation.

(c) **CENTRAL GATEWAY.**—Every proposed United States-person nomination shall pass through a single NCTC-controlled gateway for ministerial data-quality, duplication, source-integrity, and routing review before reaching the Threat Screening Center. Domestic information received solely for this purpose shall be deleted within 30 days after final disposition unless otherwise lawfully retainable.

(d) **NO NOMINATION BY ACCIDENT.**—A tip, liaison communication, suspicious-activity report, encounter report, analytic product, data feed, or intelligence report is not a nomination unless expressly designated and processed under this Act.

(e) **PRIVATE AND INFORMANT SOURCES.**—A private person has no nomination authority. Information from an anonymous source, confidential informant, former partner, family member, business competitor, employer, litigation adversary, political opponent, foreign intelligence service, paid source, or person receiving a governmental benefit may not alone establish probable cause. The Government shall independently corroborate material facts and disclose incentives, known bias, material credibility history, prior reliability, inconsistent statements, recantations, and exculpatory information.

SEC. 7. UNITED STATES TERRORIST SCREENING REVIEW PANEL.

(a) **ESTABLISHMENT.**—The Chief Justice shall designate not fewer than 21 district judges from at least 9 judicial circuits to serve staggered 7-year terms on a United States Terrorist Screening Review Panel. The Director of the Administrative Office of the United States Courts shall provide permanent clerks, secure facilities, records systems, and administrative staff.

(b) **MAGISTRATE JUDGES.**—With the consent and supervision of a panel judge, a security-cleared magistrate judge may manage scheduling, service, identity disputes, discovery logistics, and stipulated or unopposed removals, but may not enter an initial or renewed listing order.

(c) **SPECIAL ADVOCATES.**—An independent Office of Terrorist Screening Special Advocates is established in the judicial branch. Advocates shall hold appropriate clearances, be funded through the judiciary, owe no duty to the Department of Justice or a nominating agency, and test classified or withheld evidence. Appointment, compensation, removal, and ethics rules shall safeguard independence.

(d) **CONFLICTS AND RECUSAL.**—Judges, magistrate judges, and special advocates are subject to sections 455 and 144 of title 28, United States Code, as applicable, and shall disclose any material prior participation in the nomination, investigation, prosecution, or redress matter.

(e) **VENUE AND SERVICE.**—Proceedings may be conducted in the district where the person resides or is found, or remotely upon consent. The Government shall serve notice personally, by verified electronic means, or by certified mail to the last verified address; inability to locate a person despite documented diligent efforts may support substituted service ordered by the court but not indefinite secret retention.

(f) **NOTICE AND HEARING.**—Except under section 8, the Government shall give at least 14 days' notice stating the proposed category, a sufficiently specific unclassified factual basis, the person's rights, and hearing details. The person may appear through counsel, submit evidence, call witnesses, challenge reliability, and confront adverse evidence. The burden remains on the Government.

(g) **CLASSIFIED INFORMATION.**—The court may protect properly classified information only upon particularized findings. It shall provide the maximum unclassified summary consistent with national security. The judge and special advocate shall review all withheld evidence. No order may rest on evidence not tested by the special advocate.

(h) **EXCULPATORY INFORMATION.**—The Government shall disclose to the judge and special advocate all material information tending to negate probable cause, undermine source reliability, establish mistaken identity, or support a less restrictive category or removal.

(i) **WRITTEN ORDER; DURATION.**—The court shall issue findings addressing probable cause, identity, source reliability, protected activity, category criteria, and less restrictive alternatives. An order expires after one year unless renewed on a fresh showing; the prior order alone is insufficient.

(j) **PRIORITY.**—Emergency matters, mistaken-identity claims, minors' matters, and uncontested removals shall receive priority.

SEC. 8. EMERGENCY TEMPORARY LISTING.

(a) **APPLICATION.**—On certification by the Attorney General or Deputy Attorney General that advance notice would create an imminent risk of death, serious bodily injury, flight, destruction of critical evidence, or compromise of an active terrorism operation, the Government may seek an ex parte order.

(b) **STANDARD.**—The judge must find probable cause, verify minimum identifiers, and make the applicable category findings.

(c) **DURATION.**—The order expires after 72 hours. The court may extend it once for not more than 7 days upon a renewed, particularized showing. Before expiration, the Government shall provide notice and commence section 7 proceedings or the record shall be removed immediately.

SEC. 9. SPECIAL PROTECTIONS FOR MINORS.

(a) **CHILDREN UNDER 14.**—No United States person under 14 years of age may be placed in the No Fly category absent extraordinary and particularized facts establishing that the child personally is taking concrete operational steps toward conduct described in section 4(6), and clear and convincing evidence that no less restrictive measure is adequate.

(b) **PARENTAL NOTICE.**—Absent a section 8 order based on a specific risk created by notice, notice shall be served on the child's parent or legal guardian and independent counsel shall be appointed for the child.

(c) **AGES 14 THROUGH 17.**—A nomination of a person aged 14 through 17 requires corroboration from at least two materially independent sources or equivalent reliable evidence, particularized findings concerning age and capacity, and consideration of less restrictive alternatives.

(d) **NO DERIVATIVE LISTING.**—A child may not be listed solely because a parent, guardian, household member, or associate is listed.

(e) **REVIEW AT MAJORITY.**—Any order concerning a minor terminates upon the person's eighteenth birthday unless the Government obtains a new order under section 7 based on then-current evidence.

SEC. 10. SINGLE-PORTAL STATUS, CORRECTION, AND REDRESS.

(a) PUBLIC PORTAL.—The Secretary of Homeland Security, in coordination with the Attorney General, shall maintain one secure public portal for status requests, identity correction, DHS TRIP relief, Privacy Act access and amendment, and petitions under this Act. A submission through the portal exhausts no remedy and shall be routed without requiring duplicate filings.

(b) DEADLINES.—The Threat Screening Center shall acknowledge a request within 5 business days; provide a yes-or-no TSDS-status response within 15 days; correct a verified mistaken-identity match within 72 hours; and decide any other correction request within 30 days. No Glomar-type response may be given to the person who is the subject of the record.

(c) REASONS.—A listed person shall receive the category, initial-listing date, most recent judicial-authorization date, an unclassified statement of reasons, and review instructions, subject only to section 7(g).

(d) PRIVACY ACT.—The rights and duties under subsections (d), (e)(5), and (g) of section 552a of title 5, United States Code, apply to United States-person records in TSDS and derivative watchlists notwithstanding exemptions under subsections (j) or (k), with classified information protected under section 7(g).

(e) DE NOVO REVIEW.—A United States district court shall review compliance de novo, with the burden on the Government. The court may order correction, removal, downstream expungement, declaratory and injunctive relief, statutory damages under subsection (f), actual damages where proven, and reasonable attorney’s fees and costs.

(f) DAMAGES.—A United States person injured by a knowing or willful violation may recover the greater of actual damages or statutory damages of \$1,000 for each continuing course of violation, not to exceed \$50,000 per person per proceeding, and punitive damages for conduct shown by clear and convincing evidence to be malicious or in reckless disregard of rights. Economic loss is not required to recover statutory damages.

(g) ANTI-RETALIATION.—No person may be nominated, retained, repeatedly subjected to secondary screening as punishment, delayed in travel, investigated, threatened, or denied timely identity correction in retaliation for protected activity or use of any redress process. A person aggrieved may bring a civil action under subsection (e).

SEC. 11. TRANSITION REVIEW OF EXISTING RECORDS.

(a) DAYS 0 THROUGH 30.—Within 30 days after enactment, the Threat Screening Center shall remove every United States-person record that—

- (1) is a Handling Code 3 or 4 equivalent or is outside the No Fly and Selectee categories;
- (2) is not tied to an open terrorism investigation supported by documented, current facts;
- (3) lacks minimum identifiers;
- (4) has had no material terrorism-related update for 5 years; or
- (5) satisfies an automatic-removal ground under section 12.

(b) DAYS 0 THROUGH 180.—For every other legacy United States-person record, the Government shall obtain an order under section 7 within 180 days after enactment or remove the record. Applications shall be filed in staged monthly cohorts prescribed by the Panel to prevent docket concentration.

(c) NARROW EMERGENCY HOLD.—On a particularized application filed before the applicable cohort deadline, the court may retain a legacy record temporarily for not more than 30 days if probable cause and the applicable category criteria are shown and immediate removal would create an imminent and substantial risk. A hold may not be renewed except once for extraordinary cause, and the full hearing shall receive priority.

(d) NO CURE BY RECODING.—Relabeling, recoding, bulk conversion, or changing a handling instruction is not evidence and does not cure a deficient record.

(e) PUBLIC COUNTS.—At 30, 90, and 180 days, the Attorney General shall publish machine-readable counts of records reviewed, removed, renewed, denied, and held, disaggregated as required by section 15, without identifying individuals.

SEC. 12. AUTOMATIC OFF-RAMPS AND DOWNSTREAM DELETION.

(a) MANDATORY REMOVAL.—The Threat Screening Center shall remove a United States-person record within 24 hours after—

- (1) the underlying investigation closes and no current probable cause remains;
- (2) the subject is confirmed deceased;
- (3) identity is shown to belong to a different person;
- (4) a material source recants or is found unreliable and the remaining evidence does not independently establish probable cause;
- (5) a court orders removal; or
- (6) no renewal application is filed before expiration.

(b) **PROPAGATION.**—Within 3 business days, the Center shall transmit a binding, machine-readable deletion notice to every known Federal, State, local, Tribal, territorial, foreign-government, and private-sector recipient, including NCIC-connected and fusion-center systems. Domestic recipients shall certify deletion within 5 business days.

(c) **RESPONSIBILITY.**—The Director of the Threat Screening Center is legally responsible for timely propagation, verification, and audit of deletion.

(d) **NONCOMPLIANCE.**—A recipient that fails to certify deletion shall lose access immediately. Knowing continued dissemination or operational use of a deleted record is a violation subject to section 10(f), administrative discipline, contract remedies, and debarment where applicable.

SEC. 13. SHADOW-LIST AND ANTI-EVASION RULE.

(a) **COVERED SUBSTITUTE.**—No Federal agency, intelligence element, federally funded fusion center, contractor, or grantee may use a label, database, score, alert, model, or file as a substitute terrorist watchlist when it is used to impose terrorist-style aviation screening, travel consequences, officer-safety dissemination, or dissemination through TSDS, NCIC, TSA, DHS, or substantially similar channels.

(b) **PROTECTED ACTIVITY.**—No covered substitute may label a United States person a terrorist, domestic terrorist, extremist, or threat actor based solely or substantially on protected activity.

(c) **ORDINARY INVESTIGATIVE FILES.**—This section does not prohibit a lawfully predicated criminal investigation, gang-intelligence file, protective-intelligence assessment, or workplace-violence assessment that is not used to evade this Act or impose the consequences described in subsection (a).

(d) **FUSION-CENTER SCORES.**—A threat score or analytic output that ingests or infers TSDS status is covered whenever used for a purpose described in subsection (a).

(e) **MARS.**—MARS and successor defense or intelligence systems may not ingest or operationalize United States-person TSDS status except for an authorized use fully compliant with this Act. Lawful unrelated functions are unaffected.

SEC. 14. CONFORMING TSA, DHS, NCIC, AND AGENCY RULES.

(a) **CONTROLLING STANDARD.**—Notwithstanding any other law, regulation, directive, memorandum, or guidance, no Federal aviation-security, traveler-screening, redress, information-sharing, or law-enforcement dissemination authority may use a reasonable-suspicion or lower standard to place or retain a United States person in a terrorist-watchlist category.

(b) **TSA.**—The Administrator of the Transportation Security Administration shall revise all Secure Flight, No Fly, Selectee, and related procedures to conform to this Act and shall not treat TSDS status as independent authority beyond the category and duration ordered by the court.

(c) **DHS TRIP.**—The Secretary of Homeland Security shall integrate DHS TRIP into the single portal under section 10 and give correction and removal decisions binding effect across TSA, Customs and Border Protection, the Threat Screening Center, and participating systems.

(d) **NCIC.**—The Attorney General shall revise NCIC dissemination and hit-response rules so that a United States-person terrorist record is disseminated or acted upon only if supported by an unexpired order under this Act. Possible-match flags shall comply with section 5(f).

(e) **REGULATORY CONFORMITY.**—Within 60 days, each agency shall identify and suspend any contrary rule or guidance; within 180 days, it shall repeal or amend it through appropriate rulemaking. Classified guidance may not alter the public legal standard.

SEC. 15. OVERSIGHT, AUDITS, AND PUBLIC REPORTING.

(a) COORDINATED REVIEW.—At least once every 2 years, DOJ OIG, DHS OIG, the Intelligence Community Inspector General, and other relevant Inspectors General shall conduct a coordinated enterprise-wide review of nomination quality, identity accuracy, source reliability, duplicates, stale records, minors, deletion propagation, downstream uses, discrimination risks, and redress outcomes.

(b) RECIPIENT AUDITS.—Every recipient shall maintain immutable query, match, use, disclosure, correction, and deletion logs for 7 years. The relevant Inspector General may audit them without advance notice. Access shall be recertified annually.

(c) ANNUAL REPORT.—The Attorney General shall publish an unclassified, machine-readable annual report breaking out—

- (1) United States citizens, nationals, lawful permanent residents, dual nationals, and persons who naturalized after listing;
- (2) No Fly and Selectee applications, approvals, denials, renewals, expirations, and removals;
- (3) emergency orders and extensions;
- (4) minors by age band, without identifying information;
- (5) mistaken-identity cases, possible-match flags, correction times, and repeated-screening complaints;
- (6) removals for staleness and each automatic-removal ground;
- (7) status, correction, Privacy Act, and redress requests and processing times;
- (8) Federal and non-Federal recipients, access suspensions, and deletion failures; and
- (9) aggregate transition-review outcomes under section 11.

(d) GUIDANCE TO CONGRESS.—Current watchlisting guidance and every revision shall be provided to the congressional judiciary, homeland security, intelligence, and oversight committees. Legal standards governing United States persons shall be public.

SEC. 16. APPROPRIATIONS AND ADMINISTRATION.

(a) AUTHORIZATION.—There are authorized to be appropriated such sums as may be necessary for fiscal years 2027 through 2031 to the Federal judiciary for the Panel, permanent staff, secure facilities, and independent special advocates; and to the Inspectors General and Comptroller General for audits required by this Act.

(b) SEPARATE FUNDING.—Funds for special advocates shall be appropriated to the judiciary and may not be controlled, withheld, or conditioned by the Department of Justice or a nominating agency.

(c) TECHNOLOGY.—Appropriations may be used for the public portal, interoperable identity-resolution services, immutable audit logs, and machine-readable correction and deletion infrastructure.

SEC. 17. DISCIPLINE, WHISTLEBLOWERS, AND RULEMAKING.

(a) DISCIPLINE.—Knowing and willful circumvention, falsification, retaliatory use, or failure to remove or propagate deletion is grounds for administrative discipline up to removal, without limiting civil or criminal liability.

(b) WHISTLEBLOWERS.—A lawful disclosure to Congress, an Inspector General, or authorized oversight body concerning unlawful watchlisting or deletion failure is protected under applicable Federal whistleblower law. No nondisclosure agreement may bar such a disclosure.

(c) RULEMAKING.—The Attorney General, Secretary of Homeland Security, and Director of National Intelligence shall issue an interim rule within 60 days and a final rule within 180 days. Regulations may not delay or narrow rights created by this Act.

SEC. 18. CONFORMING AMENDMENT REGARDING NCTC.

Section 119(e) of the National Security Act of 1947 (50 U.S.C. 3056(e)) is amended to authorize NCTC to receive exclusively domestic United States-person information solely for the temporary ministerial, duplication, identity-

quality, source-integrity, and routing review required by section 6(c), without authority to direct a domestic investigation and subject to mandatory deletion.

SEC. 19. SEVERABILITY.

If any provision of this Act, or its application to any person or circumstance, is held invalid, the remainder and its application to other persons or circumstances shall not be affected.

SEC. 20. EFFECTIVE DATE.

This Act takes effect on enactment. New nominations must comply immediately; legacy records are governed by section 11. Rights to status, correction, anti-retaliation protection, and automatic removal are not delayed by rulemaking.

APPENDIX A — IMPLEMENTATION AND OVERSIGHT CROSSWALK

This appendix is explanatory material for congressional distribution and is not part of the proposed statutory text.

- Staged legacy cleanup: automatic 30-day removals; court-supervised review within 180 days; narrow emergency holds; public outcome counts. (Secs. 11–12.)
- Defined categories and preventive probable cause: express No Fly and Selectee criteria; concrete operational steps; specified terrorism and material-support statutes; protected activity excluded. (Secs. 4–5.)
- Mistaken identity and minors: minimum identifiers, non-listing possible-match mechanism, rapid correction, special rules for children, and review at age 18. (Secs. 5, 9–10.)
- Workable judiciary: 21 judges across 9 circuits, permanent staff, independent special advocates, magistrate support, venue, service, and conflict rules. (Sec. 7.)
- Downstream accountability: narrow permissible uses, written recipient agreements, audit logs, annual recertification, machine-readable deletion, and immediate cutoff for noncompliance. (Secs. 5, 12, 15.)
- Effective remedies: response deadlines, de novo review, statutory and actual damages, fees, and an enforceable anti-retaliation right. (Sec. 10.)
- Anti-evasion precision: terrorist-style consequences and screening channels are covered; ordinary lawful criminal and safety files are preserved. (Sec. 13.)
- Operational conformity and funding: TSA, DHS TRIP, NCIC, and inconsistent agency guidance are conformed; judges, advocates, audits, portal, and deletion systems are authorized for funding. (Secs. 14, 16–18.)

APPENDIX B — SOURCE-VERIFICATION AND DRAFTING NOTES

These notes identify requested assertions that should not be presented to Congress as established fact. The proposed bill addresses the underlying policy concern where a defensible statutory solution is available.

- (1) “97% are non-investigative subjects / do not meet reasonable suspicion.” — The cited OIG record does not establish that proposition. Audit 05-27 found that 96.68% of a 109,849-record subset was in Handling Codes 3 and 4, the two lowest handling categories. Audit 09-25 separately discussed non-investigative subjects. The reports do not equate the two concepts and do not conclude that 97% of all watchlisted persons lacked reasonable suspicion. The bill therefore uses the verified handling-code statistics and the separate verified findings on non-investigative-subject controls.
- (2) “Anyone, including a scorned former partner or business competitor, can nominate a victim.” — Current FBI public guidance states that only government agencies can nominate a person to the federal terrorism watchlist. [29] The bill instead addresses the real risk that biased private allegations can enter government channels by requiring corroboration, source-reliability disclosure, and governmental/judicial review.
- (3) “Probable cause is the minimum constitutional requirement.” — That statement is not consistent with existing appellate authority. The Peters report cites *Kashem v. Barr* for the proposition that reasonable suspicion satisfies due process.[30] Congress can nevertheless enact probable cause as a higher statutory safeguard. The bill intentionally does so and describes it as a congressional policy judgment, not a settled constitutional minimum.
- (4) “The 2024 overnight conversion of non-investigative subjects into reasonable-suspicion terrorists was illegal.” — I did not locate an authoritative public source establishing a mass 2024 conversion matching that description. The bill therefore orders a joint audit of any bulk recategorization since January 1, 2023 and expressly provides that recoding or relabeling cannot substitute for individualized probable cause.
- (5) “MARS is a database replicating the TSIDS.” — Public Department of Defense budget material confirms the existence of MARS, but the primary sources reviewed do not establish that it is a TSIDS replica.[31] The bill prohibits MARS or any other system from being used to mirror or operationalize United States-person TSIDS status outside the safeguards of the Act and requires an independent audit.
- (6) “The FBI has been exposed as corrupt, so corrupt agents must be stripped of power.” — For bipartisan legislative drafting, the bill does not characterize the FBI as an institution as corrupt. It instead removes unchecked discretion through mandatory headquarters review, a centralized nomination gateway, Article III authorization, expiring orders, redress, and external audits. These protections apply regardless of administration or political control.
- (7) Requested statement questioning whether terrorists or airplanes were involved in the September 11 attacks. — This draft does not include that assertion. The established evidentiary and historical record documents the hijacking of four commercial aircraft by al-Qaeda terrorists. Including a contrary factual finding would be unsupported and would materially undermine the credibility and bipartisan viability of the proposed legislation. The bill preserves the requested 25th-anniversary framing by stating that Congress should now reevaluate and codify post-9/11 watchlisting powers.
- (8) “Handling Codes 3 and 4 are the list for victims of government weaponization.” — The OIG audits do not make that finding. The bill nevertheless eliminates legacy Handling Code 3/4 or equivalent non-No-Fly/non-Selectee status for United States persons because such consequential watchlisting should satisfy a defined statutory standard and review process.

APPENDIX C — PRINCIPAL AUTHORITIES

- (1) Homeland Security Presidential Directive 6, Integration and Use of Screening Information (Sept. 16, 2003).
- (2) DOJ OIG, Review of the Terrorist Screening Center, Audit Report 05-27 (June 2005).
- (3) DOJ OIG, Follow-up Audit of the Terrorist Screening Center, Audit Report 07-41 (Sept. 2007).
- (4) DOJ OIG, Audit of the U.S. Department of Justice Terrorist Watchlist Nomination Processes, Audit Report 08-16 (Mar. 2008).
- (5) DOJ OIG, The Federal Bureau of Investigation’s Terrorist Watchlist Nomination Practices, Audit Report 09-25 (May 2009).
- (6) DOJ OIG, Audit of the Federal Bureau of Investigation’s Management of Terrorist Watchlist Nominations, Audit Report 14-16 (Mar. 25, 2014).
- (7) U.S. Senate Committee on Homeland Security and Governmental Affairs, Majority Staff, *Mislabeled as a Threat: How the Terrorist Watchlist & Government Screening Practices Impact Americans* (Dec. 2023).
- (8) FBI, Overview of the U.S. Government’s Terrorist Watchlisting Process and Procedures (Apr. 2024).
- (9) FBI, Threat Screening Center public guidance and March 19, 2025 name-change announcement.
- (10) 50 U.S.C. 3056 (National Counterterrorism Center).

[1] Homeland Security Presidential Directive 6, “Integration and Use of Screening Information,” Sept. 16, 2003 (directing the Attorney General to establish a consolidated screening organization, requiring safeguards for U.S. persons, and requiring implementation consistent with the Constitution and applicable law), archived at georgewbush-whitehouse.archives.gov/news/releases/2003/09/20030916-5.html.

[2] Federal Bureau of Investigation, “The Terrorist Screening Center Changes Name to the Threat Screening Center,” Mar. 19, 2025 (renaming the TSC to reflect an expanded mission).

[3] Homeland Security Presidential Directive 6, “Integration and Use of Screening Information,” Sept. 16, 2003 (directing the Attorney General to establish a consolidated screening organization, requiring safeguards for U.S. persons, and requiring implementation consistent with the Constitution and applicable law), archived at georgewbush-whitehouse.archives.gov/news/releases/2003/09/20030916-5.html.

[4] U.S. Department of Justice, Office of the Inspector General, Review of the Terrorist Screening Center, Audit Report 05-27 (June 2005), Executive Summary. In a subset of 109,849 records, Handling Code 3 represented 22.04% and Handling Code 4 represented 74.64%; the OIG described them as the two lowest categories and noted that Handling Code 4 could include associates who may not pose a direct terrorist threat. The OIG also identified inconsistent and missing handling-code data.

[5] U.S. Department of Justice, Office of the Inspector General, Review of the Terrorist Screening Center, Audit Report 05-27 (June 2005), Executive Summary. In a subset of 109,849 records, Handling Code 3 represented 22.04% and Handling Code 4 represented 74.64%; the OIG described them as the two lowest categories and noted that Handling Code 4 could include associates who may not pose a direct terrorist threat. The OIG also identified inconsistent and missing handling-code data.

[6] U.S. Department of Justice, Office of the Inspector General, Follow-up Audit of the Terrorist Screening Center, Audit Report 07-41 (Sept. 2007), Executive Summary and Findings. The OIG reported duplicate records, incompatible database versions, an FBI bypass process, errors or inconsistencies in 38% of 105 routinely reviewed records, and that 45% of positive-match redress records referred for review required modification or removal.

[7] U.S. Department of Justice, Office of the Inspector General, Follow-up Audit of the Terrorist Screening Center, Audit Report 07-41 (Sept. 2007), Executive Summary and Findings. The OIG reported duplicate records, incompatible database versions, an FBI bypass process, errors or inconsistencies in 38% of 105 routinely reviewed records, and that 45% of positive-match redress records referred for review required modification or removal.

[8] U.S. Department of Justice, Office of the Inspector General, Audit of the U.S. Department of Justice Terrorist Watchlist Nomination Processes, Audit Report 08-16 (Mar. 2008), at 3, 10-13, 22-24. The OIG found incomplete or inaccurate field submissions, direct field-to-NCTC nominations bypassing headquarters review, weak controls over non-investigative-subject nominations, and information-sharing records treated as nominations without adequate source-agency awareness or maintenance controls.

[9] U.S. Department of Justice, Office of the Inspector General, Audit of the U.S. Department of Justice Terrorist Watchlist Nomination Processes, Audit Report 08-16 (Mar. 2008), at 3, 10-13, 22-24. The OIG found incomplete

or inaccurate field submissions, direct field-to-NCTC nominations bypassing headquarters review, weak controls over non-investigative-subject nominations, and information-sharing records treated as nominations without adequate source-agency awareness or maintenance controls.

[10] U.S. Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation’s Terrorist Watchlist Nomination Practices, Audit Report 09-25 (May 2009), Results in Brief and Part IV. Among the reviewed samples, the OIG found 15% of terrorism investigations lacked required nominations, 78% of initial nominations were untimely, 67% of required modifications were not made, 8% of closed cases were not removed as required, and 72% were not timely removed; it also found weak or nonexistent controls over non-standard nomination processes, through which more than 62,000 nominations had been made.

[11] U.S. Department of Justice, Office of the Inspector General, The Federal Bureau of Investigation’s Terrorist Watchlist Nomination Practices, Audit Report 09-25 (May 2009), Results in Brief and Part IV. Among the reviewed samples, the OIG found 15% of terrorism investigations lacked required nominations, 78% of initial nominations were untimely, 67% of required modifications were not made, 8% of closed cases were not removed as required, and 72% were not timely removed; it also found weak or nonexistent controls over non-standard nomination processes, through which more than 62,000 nominations had been made.

[12] Statement of Michael E. Horowitz, Inspector General, U.S. Department of Justice, before the Senate Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies (2014), summarizing Audit Report 14-16 as finding that FBI time requirements could be strengthened and identifying weaknesses in the database used to submit, monitor, and track non-investigative-subject nominations; see also DOJ OIG, Audit Report 14-16 (Mar. 25, 2014).

[13] U.S. Senate Committee on Homeland Security and Governmental Affairs, Majority Staff, *Mislabeled as a Threat: How the Terrorist Watchlist & Government Screening Practices Impact Americans* (Dec. 2023), Findings of Fact 1-6. The report identified at least 22 screening mechanisms, approximately 1.8 million terrorist-watchlist records as of Nov. 2022, more than 500 private-sector entities with access to a subset, and significant transparency and redress concerns.

[14] U.S. Senate Committee on Homeland Security and Governmental Affairs, Majority Staff, *Mislabeled as a Threat: How the Terrorist Watchlist & Government Screening Practices Impact Americans* (Dec. 2023), Findings of Fact 1-6. The report identified at least 22 screening mechanisms, approximately 1.8 million terrorist-watchlist records as of Nov. 2022, more than 500 private-sector entities with access to a subset, and significant transparency and redress concerns.

[15] *Id.*, Recommendations 1-6 and Part VIII. The report recommended a coordinated full-scope Inspector General review, meaningful redress, annual reporting, and evaluation of constitutional protections, and concluded that fragmented oversight had prevented a comprehensive and consistent independent assessment.

[16] *Id.* at Part V.C & n.145 (discussing concerns about the reasonable-suspicion standard and citing *Kashem v. Barr*, 941 F.3d 358 (9th Cir. 2019), as holding the standard satisfies due process). The probable-cause requirement in this draft is therefore framed as a higher statutory safeguard.

[17] *Mislabeled as a Threat*, Part VI.B-C (discussing *Latif v. Holder*, 28 F. Supp. 3d 1134 (D. Or. 2014), which found the then-existing No-Fly redress process constitutionally deficient, and revised DHS TRIP procedures adopted afterward).

[18] *Mislabeled as a Threat*, Part VI.C, “Timeline of Notable Watchlist Cases” (summarizing *Ibrahim v. DHS*, 62 F. Supp. 3d 909 (N.D. Cal. 2014), involving mistaken No-Fly placement caused by an FBI agent’s form error).

[19] Federal Bureau of Investigation, Threat Screening Center, “Privacy and Civil Liberties: Nominations” (current public guidance stating that only government agencies can nominate and that race, ethnicity, religion, First Amendment-protected activity, guesses, and hunches cannot by themselves be the basis for watchlisting).

[20] Letter from Sen. Edward J. Markey to ICE Acting Director Todd Lyons (Feb. 3, 2026) (seeking confirmation or denial after an ICE officer reportedly told a peaceful observer that her information would be placed in a “nice little database” labeling her a domestic terrorist). The draft treats this as an oversight allegation, not a proven description of an ICE system.

[21] Department of Defense, Defense Information Systems Agency, FY 2027 RDT&E Budget Justification, PE 0303150K, identifying the “Machine-assisted Analytic Rapid-repository System (MARS).” The public primary sources reviewed for this draft do not establish that MARS is a replica of the TSDS.

[22] Federal Bureau of Investigation, “The Terrorist Screening Center Changes Name to the Threat Screening Center,” Mar. 19, 2025 (renaming the TSC to reflect an expanded mission).

[23] 50 U.S.C. § 3056(d)-(e) (defining NCTC’s missions and limitations concerning exclusively domestic terrorism intelligence). Section 16 of this draft creates only a narrow ministerial/quality-control exception for routing domestic U.S.-person watchlist nominations and expressly denies NCTC operational control over domestic investigations.

[24] U.S. Department of Justice, Office of the Inspector General, Audit of the U.S. Department of Justice Terrorist Watchlist Nomination Processes, Audit Report 08-16 (Mar. 2008), at 3, 10-13, 22-24. The OIG found incomplete or inaccurate field submissions, direct field-to-NCTC nominations bypassing headquarters review, weak controls over non-investigative-subject nominations, and information-sharing records treated as nominations without adequate source-agency awareness or maintenance controls.

[25] Department of Defense, Defense Information Systems Agency, FY 2027 RDT&E Budget Justification, PE 0303150K, identifying the “Machine-assisted Analytic Rapid-repository System (MARS).” The public primary sources reviewed for this draft do not establish that MARS is a replica of the TSDS.

[26] Federal Bureau of Investigation, Threat Screening Center, “Privacy and Civil Liberties: Nominations” (current public guidance stating that only government agencies can nominate and that race, ethnicity, religion, First Amendment-protected activity, guesses, and hunches cannot by themselves be the basis for watchlisting).

[27] *Id.*, Recommendations 1-6 and Part VIII. The report recommended a coordinated full-scope Inspector General review, meaningful redress, annual reporting, and evaluation of constitutional protections, and concluded that fragmented oversight had prevented a comprehensive and consistent independent assessment.

[28] 50 U.S.C. § 3056(d)-(e) (defining NCTC’s missions and limitations concerning exclusively domestic terrorism intelligence). Section 16 of this draft creates only a narrow ministerial/quality-control exception for routing domestic U.S.-person watchlist nominations and expressly denies NCTC operational control over domestic investigations.

[29] Federal Bureau of Investigation, Threat Screening Center, “Privacy and Civil Liberties: Nominations” (current public guidance stating that only government agencies can nominate and that race, ethnicity, religion, First Amendment-protected activity, guesses, and hunches cannot by themselves be the basis for watchlisting).

[30] *Id.* at Part V.C & n.145 (discussing concerns about the reasonable-suspicion standard and citing *Kashem v. Barr*, 941 F.3d 358 (9th Cir. 2019), as holding the standard satisfies due process). The probable-cause requirement in this draft is therefore framed as a higher statutory safeguard.

[31] Department of Defense, Defense Information Systems Agency, FY 2027 RDT&E Budget Justification, PE 0303150K, identifying the “Machine-assisted Analytic Rapid-repository System (MARS).” The public primary sources reviewed for this draft do not establish that MARS is a replica of the TSDS.