

119TH CONGRESS
2D SESSION

H. R. 9887

To establish a registry to reduce swatting, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 22, 2026

Mr. WALKINSHAW (for himself and Ms. LEE of Florida) introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To establish a registry to reduce swatting, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Swatting Registry Best
5 Practices Act”.

6 **SEC. 2. DEVELOPMENT AND ISSUANCE OF GUIDANCE ON**
7 **SWATTING REGISTRIES.**

8 (a) IN GENERAL.—Not later than 1 year after the
9 date of the enactment of this Act, the Attorney General,
10 in consultation with the Secretary of Homeland Security,
11 shall develop and issue guidance, which shall include best

1 practices for State, Tribal, territorial, and local govern-
2 ments and public safety agencies regarding the establish-
3 ment, operation, and oversight of voluntary swatting reg-
4 istries and related public safety protocols.

5 (b) CONSULTATION.—In developing the guidance
6 under subsection (a), the Attorney General shall consult
7 with—

8 (1) State, local, Tribal, and territorial law en-
9 forcement agencies and public safety answering
10 points, including those serving large, mid-sized, and
11 rural jurisdictions;

12 (2) public safety, emergency communications,
13 and 9–1–1 system experts with experience in call-
14 taking, dispatch, computer-aided dispatch systems,
15 and incident response protocols;

16 (3) privacy, cybersecurity, data governance, and
17 civil liberties experts with demonstrated technical ex-
18 pertise in the secure design, operation, oversight,
19 and auditing of sensitive public safety databases;

20 (4) disability access, language access, and vic-
21 tim services experts with demonstrated expertise in
22 ensuring voluntary registry programs are accessible
23 to individuals who may face elevated risks of swat-
24 ting or targeting harassment;

1 (5) technology providers and 9–1–1 system ven-
2 dors with relevant expertise in secure database de-
3 sign, caller authentication, and call-handling proto-
4 cols; and

5 (6) individuals and households who have been
6 victims of swatting incidents.

7 (c) GUIDANCE.—

8 (1) CONTENTS.—The guidance required under
9 subsection (a) shall include, at a minimum, the fol-
10 lowing:

11 (A) PROGRAM DESIGN AND ELIGIBILITY.—

12 The best practices for designing voluntary swat-
13 ting registries that—

14 (i) allow voluntary opt-in by residents;

15 (ii) identify categories of higher-risk
16 registrants, including individuals reason-
17 ably believed to face an elevated risk of
18 swatting or targeting harassment;

19 (iii) provide clear criteria and proce-
20 dures for registration, renewal, and re-
21 moval; and

22 (iv) ensure equitable access for com-
23 munities with limited English proficiency,
24 persons with disabilities, and other under-
25 served groups.

1 (B) DATA ELEMENTS AND DATA MINIMIZA-
2 TION.—The best practices regarding the nec-
3 essary data elements to be collected and stored,
4 which may include—

5 (i) the address and, where applicable,
6 unit or apartment number;

7 (ii) primary and secondary telephone
8 numbers;

9 (iii) additional contact methods such
10 as email addresses or other secure,
11 verifiable communication channels;

12 (iv) optional verification mechanisms,
13 such as pre-agreed code words or phrases,
14 and contact information for multiple
15 household members; and

16 (v) associated time frames or condi-
17 tions (such as expected periods of height-
18 ened risk), where applicable, while mini-
19 mizing the collection and retention of per-
20 sonally identifiable information.

21 (C) INCIDENT RESPONSE INTEGRATION.—
22 The best practices for integrating registry infor-
23 mation into call-taking and dispatch workflows,
24 including—

1 (i) automated dispatch flags or alerts
2 when a call originates from, or concerns, a
3 registered address;

4 (ii) guidance for tactical response ad-
5 justments when verification suggests a
6 likely hoax, including options for lower-es-
7 calation approaches such as staged re-
8 sponses, announcements, or requests for
9 occupants to meet officers outside when
10 safe to do so; and

11 (iii) protocols for documentation and
12 after-action review of incidents involving
13 registered addresses.

14 (D) OFFICER SAFETY AND TRAINING.—
15 Recommendations for training call-takers, dis-
16 patch personnel, and responding officers on—

17 (i) the nature and risks of swatting;

18 (ii) appropriate use of swatting reg-
19 istry information in assessing risk and se-
20 lecting tactics; and

21 (iii) avoiding overreliance on
22 unverified registry data while using such
23 data to reduce unnecessary risk.

1 (E) PRIVACY, CIVIL RIGHTS, AND CIVIL
2 LIBERTIES PROTECTIONS.—The best practices
3 to—

4 (i) ensure participation is voluntary
5 and based on informed consent;

6 (ii) restrict access to registry data to
7 authorized personnel, with role-based ac-
8 cess controls;

9 (iii) require encryption of records at
10 rest and in transit, and other appropriate
11 cybersecurity safeguards;

12 (iv) provide full audit logging of ac-
13 cess and use;

14 (v) prevent misuse of registry infor-
15 mation for discriminatory or retaliatory
16 purposes; and

17 (vi) provide notice, redress, and com-
18 plaint mechanisms for registrants and the
19 public.

20 (F) DATA RETENTION, ACCURACY, AND
21 GOVERNANCE.—The best practices regarding—

22 (i) reasonable limits on data retention;

23 (ii) procedures for registrants to up-
24 date or delete their information at any
25 time;

(iii) periodic review and renewal mechanisms, including annual prompts or other methods to ensure accuracy; and

(iv) appropriate governance, including designation of responsible officers, policy review cycles, and community engagement.

(G) TECHNOLOGY, INTEROPERABILITY, AND FUNDING CONSIDERATIONS.—Recommendations regarding—

(i) technical approaches for integrating swatting registries with existing 9–1–1 and computer-aided dispatch systems;

(ii) secure online portals or mechanisms for registration and updates;

(iii) scalability for small and resource-constrained jurisdictions; and

(iv) potential Federal resources, including existing grant programs, that may support implementation.

(H) METRICS AND EVALUATION.—Recommended metrics and methodologies to evaluate—

(i) impact on safety outcomes for residents, pets, and officers;

(ii) impact on property damage, use-of-force incidents, and traumatic forced entries;

(iii) impact on litigation exposure and settlement costs; and

(iv) impact on operational efficiency and deterrence of swatting.

(I) USE BEYOND SWATting.—Considerations for how registry information, if appropriately designed and consented to, may safely assist in other types of emergencies (such as medical crises or wellness checks), while maintaining clear limitations and safeguards to prevent overcollection or misuse.

(d) PUBLIC AVAILABILITY.—The Attorney General shall make the guidance issued under this subsection publicly available on the website of the Department of Justice, except for any material that would disclose information that is sensitive or classified.

(e) UPDATES.—The Attorney General may periodically update the guidance issued under this subsection as appropriate, including to reflect technological developments, emerging threats, and lessons learned from State, Tribal, territorial, and local implementation.

1 **SEC. 3. TECHNICAL ASSISTANCE AND DISSEMINATION.**

2 (a) TECHNICAL ASSISTANCE.—Subject to the avail-
3 ability of appropriations, the Attorney General may pro-
4 vide technical assistance to State, Tribal, territorial, and
5 local public safety agencies seeking to—

6 (1) establish voluntary swatting registries con-
7 sistent with the guidance issued under section 4; or

8 (2) integrate swatting-related verification and
9 response protocols into existing 9–1–1 and dispatch
10 operations.

11 (b) USE OF EXISTING PROGRAMS.—The Attorney
12 General shall, to the maximum extent practicable, use ex-
13 isting grant and assistance programs administered by the
14 Department of Justice to disseminate the guidance issued
15 under this Act and to support eligible jurisdictions that
16 choose to design or implement swatting registries con-
17 sistent with such guidance.

18 **SEC. 4. RULES OF CONSTRUCTION.**

19 Nothing in this Act may be construed to—

20 (1) authorize the creation or maintenance of a
21 Federal swatting registry;

22 (2) require any State, Tribal, territorial, or
23 local government to establish a swatting registry;
24 and

1 (3) limit the discretion of responding law en-
2 forcement officers to take actions reasonably nec-
3 essary to protect life and public safety.

4 **SEC. 5. DEFINITIONS.**

5 In this Act:

6 (1) SWATTING.—The term “swatting” means
7 the knowing and intentional making of a false or
8 misleading report to a public safety answering point,
9 law enforcement agency, or emergency service, con-
10 cerning an alleged ongoing emergency or threat,
11 with the reasonably foreseeable result of prompting
12 an armed or otherwise heightened law enforcement
13 response to a person or address.

14 (2) SWATTING REGISTRY.—The term “swatting
15 registry” means a voluntary program or database
16 maintained by a State, Tribal, territorial, or local
17 public safety or law enforcement agency that—

18 (A) allows individuals at an elevated risk
19 of swatting to register an address and associ-
20 ated contact information;

21 (B) stores such information in a secure,
22 access-controlled system available to authorized
23 dispatchers and supervisory personnel; and

1 (C) is designed to support verification and
2 response protocols when an emergency call is
3 received for a registered address.

4 (3) PUBLIC SAFETY ANSWERING POINT.—The
5 term “public safety answering point” has the mean-
6 ing given that term in section 222(h) of the Commu-
7 nications Act of 1934 (47 U.S.C. 222(h)).

○