

3rd United States Congress
5th Session

S. 16

to deter and punish terrorist acts in the United States, to combat organized crime, to enhance law enforcement investigatory tools, and for other purposes.

IN THE SENATE OF THE UNITED STATES
January 5th, 2022

Mr. YANG(for himself, for Mr. SOUTHERNSHERIFF, author)
introduced the following resolution, which was referred to the floor.

A BILL

to deter and punish terrorist acts in the United States, to combat organized crime, to enhance law enforcement investigatory tools, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the
United States of America Assembled.*

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Countering, Restricting, and other Appropriate Controls for Killers (CRACK) Act of 2022”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title and table of contents.

Sec. 2. Construction; severability.

GROUP A—ENHANCING DOMESTIC SECURITY

TITLE I—ENHANCING NATIONAL SECURITY AUTHORITIES

Subtitle A—Adjusting National Security Coordination

Subtitle C—Enhancement of Law Enforcement Investigative Tools

TITLE II—PROTECTING NATIONAL SECURITY INFORMATION

Subtitle A—Safeguarding Classified Information

Subtitle B—Protected Information Otherwise

TITLE III—ENHANCING INVESTIGATIONS OF TERRORIST PLOTS

Subtitle A—Facilitating Information Sharing and Cooperation

TITLE IV—ENHANCING PROSECUTION AND PREVENTION OF TERRORIST CRIMES

Subtitle A—Increasing Penalties and Protections Against Terrorist Acts

Subtitle B—Incapacitating Terrorism Financing

GROUP B—COMBATTING ORGANIZED CRIME

TITLE V—STRENGTHENING CRIMINAL INTELLIGENCE

TITLE VI—ADAPTING TO RACKETEERING INFLUENCED AND CRIMINAL ORGANIZATIONS

TITLE VII—MISCELLANEOUS PROVISIONS

SECTION 2. CONSTRUCTION; SEVERABILITY.

Severability. — Any provision of this Act held to be invalid or unenforceable by its terms, or as applied to any person or circumstance, shall be construed so as to give it the maximum effect permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which event such provision shall be deemed severable from this Act and shall not affect the remainder thereof or the application of such provision to other persons not similarly situated or to other, dissimilar circumstances.

GROUP A—ENHANCING DOMESTIC SECURITY

TITLE I—ENHANCING NATIONAL SECURITY AUTHORITIES

Subtitle A—Reforming National Security Coordination

SECTION 101. NATIONAL SECURITY ACT REFORM.

The National Security Act of 2021 shall be repealed in its entirety.

SECTION 102. NATIONAL SECURITY COUNCIL.

- (a) ***National Security Council.*** There is a council known as the National Security Council (in this section referred to as the “Council” or the “NSC”).
- (b) ***Functions.*** Consistent with the direction of the President, the functions of the Council shall be to—
 - (i) advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the Armed Forces and the other departments and agencies of the United States Government to cooperate more effectively in matters involving the national security;
 - (ii) assess and appraise the objectives, commitments, and risks of the United States in relation to the actual and potential military power of the United States, and make recommendations thereon to the President;

- (iii) make recommendations to the President concerning policies on matters of common interest to the departments and agencies of the United States Government concerned with the national security; and
 - (iv) coordinate, without assuming operational authority, the United States Government response to malign foreign influence operations and campaigns.
- (c) **Membership.**
- (i) ***In General.*** The Council consists of the President, the Vice President, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of the Treasury, the Assistant to the President for National Security Affairs, and such other officers of the United States Government as the President may designate.
 - (ii) ***Attendance and participation in meetings.*** The President may designate such other officers of the United States Government as the President considers appropriate, including the Director of National Intelligence, and the Chairman of the Joint Chiefs of Staff to attend and participate in meetings of the Council.
- (d) ***Presiding Officer.*** At meetings of the Council, the President shall preside or, in the absence of the President, a member of the Council designated by the President shall preside.
- (e) ***Congressional Briefing.*** No less frequently than twice a month, the Assistant to the President for National Security Affairs, or the Director of National Intelligence, shall provide to the congressional committees specified in subparagraphs (i) and (ii) a briefing on the activities of the National Security Council.
- (i) The Committees on Armed Services, Foreign Affairs, and Oversight and Government Reform, and the Permanent Select Committee on Intelligence, or any successor committees, of the House of Representatives.
 - (ii) The Committees on Armed Services, Foreign Relations, and Homeland Security and Governmental Affairs, and the Select Committee on Intelligence, or any successor committees, of the Senate.

SECTION 103. NATIONAL SECURITY THREATS.

- (a) ***Prohibition on Employment.*** No person shall be eligible for employment, services, or support from the United States Intelligence Community who is a national security threat to the integrity of the national security apparatus.

(b) ***Designation of Entities Subject to Prohibition.***

- (i) When the National Security Council determines, either *sua sponte* or in response to a petition from the Director of National Intelligence, that a person poses a national security threat to the integrity of the national security apparatus, the NSC shall issue a public notice advising that such designation has been proposed as well as the basis for such designation.
- (ii) Upon issuance of such notice, interested parties may file comments responding to the initial designation, including proffering an opposition to the initial designation. If the initial designation is unopposed, the entity shall be deemed to pose a national security threat five days after the issuance of the notice. If any party opposes the initial designation, the designation shall take effect only if the NSC determines that the affected entity should nevertheless be designated as a national security threat to the integrity of the national security apparatus. In either case, the NSC shall issue a second public notice announcing its final designation and the effective date of its final designation. The NSC shall make a final designation no later than seven days after the release of its initial determination notice. NSC may, however, extend such deadlines for good cause.
- (iii) The NSC will act to reverse its designation upon a finding that an entity is no longer a threat to the integrity of the national security apparatus. A designated party, or any other interested party, may submit a petition asking the NSC to remove a designation. The NSC shall seek the input of Executive Branch agencies upon receipt of such a petition. If the record shows that a designated party is no longer a national security threat, the NSC shall promptly issue an order reversing its designation of that party. The NSC may dismiss repetitive or frivolous petitions for reversal of a designation without notice and comment. If the NSC reverses its designation, the NSC shall issue an order announcing its decision along with the basis for its decision.
- (iv) The NSC shall have the discretion to revise this process or follow a different process if appropriate to the circumstances, consistent with providing affected parties an opportunity to respond and with any need to act expeditiously in individual cases.

(c) ***Congressional Oversight.*** The Director of National Intelligence shall furnish all information relating to a designation of a national security threat to the integrity of the national security apparatus to the homeland security and intelligence committees of Congress who may, individually or jointly, enjoin the National

Security Council from designating a party as a national security threat to the integrity of the national security apparatus.

- (d) **Definitions.** In this section, the term “national security apparatus” means a telecommunications or information system, or other critical infrastructure operated by the Federal Government, the function, operation, or use of which—
- (i) involves intelligence activities;
 - (ii) involves cryptologic activities related to national security;
 - (iii) involves command and control of military forces;
 - (iv) involves equipment that is an integral part of a weapon or weapons system; or
 - (v) is critical to the direct fulfillment of military or intelligence missions.

SECTION 104. ACCESS TO INTELLIGENCE.

Unless otherwise directed by the President, the members of the National Security Council shall have access to all national intelligence and intelligence related to the national security for any matter brought to the National Security Council.

SECTION 105. SECURITY COUNCIL COMMUNICATIONS.

The President and the National Security Advisor shall ensure that communications within any National Security Council communication system are limited to the official business of the National Security Council.

Subtitle B—Enhancement of Law Enforcement Investigative Tools

SECTION 150. DEFINITION OF TERRORIST ACTIVITIES.

- (a) Section 2510 of title 18, United States Code, is amended—
- (i) by redesignating paragraphs (20) and (21) as paragraphs (22) and (23) respectively; and
 - (ii) by inserting after paragraph (19) the following:
 - “(20) ‘terrorist activities’ means an offense described in section 2332b(g)(5)(B), an offense involved in or related to domestic or international terrorism as defined in section 2331, or a conspiracy or attempt to engage in such conduct;
 - “(21) ‘criminal investigation’ includes any investigation of terrorist activities;”.
- (b) Section 3127(1) of title 18, United States Code, is amended by inserting “‘terrorist activities’, ‘criminal investigation’,” after “service”,

SECTION 151. RESERVED.

Reserved.

SECTION 152. RESERVED.

Reserved.

SECTION 153. ADMINISTRATIVE SUBPOENAS IN TERRORISM INVESTIGATIONS.

- (a) IN GENERAL— Chapter 113B of title 18, United States Code, is amended by inserting after section 2332i the following:

“Sec. 2332j. Administrative subpoenas in terrorism investigations.

- (a) AUTHORIZATION OF USE—In any investigation with respect to an offense listed in section 2332b(g)(5)(B) or an offense involved in or related to international or domestic terrorism as defined in section 2331, the Attorney General may subpoena witnesses, compel the attendance and testimony of witnesses, and require the production of any records (including books, papers, documents, electronic data, and other tangible things that constitute or contain evidence) that he finds relevant or material to the investigation. A subpoena under this section shall describe the records or items required to be produced and prescribe a return date within a reasonable period of time within which records or items can be assembled and made available. The attendance of witnesses and the production of records may be required from any place at any designated place of hearing.
- (b) SERVICE— A subpoena issued under this section may be served by any person designated in the subpoena as the agent of service. Service upon a natural person may be made by personal delivery of the subpoena to him. Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association that is subject to suit under a common name, by delivering the subpoena to an officer, to a managing or general agent, or to any other agent authorized by appointment, or by law to receive service of process. The affidavit of the person serving the subpoena entered by him on a true copy thereof shall be sufficient proof of service.
- (c) ENFORCEMENT—In the case of the contumacy by, or refusal to obey a subpoena issued to, any person, the Attorney General may invoke the aid of any court of the United States within whose jurisdiction the investigation is carried on or the subpoenaed person resides, carries on business, or may be found, to compel compliance with the subpoena. The

court may issue an order requiring the subpoenaed person, in accordance with the subpoena, to appear, to produce records, or to give testimony touching the matter of the investigation. Any failure to obey the order of the court may be punished by the court as contempt thereof.

- (d) NON-DISCLOSURE REQUIREMENTS—No person shall disclose to any other person that a subpoena was received or records provided pursuant to this section, other than to (i) those persons to whom such disclosure is necessary in order to comply with the subpoena, (ii) an attorney to obtain legal advice with respect to testimony or the production of records in response to the subpoena, and (iii) other persons as permitted by the Attorney General. Any person who receives a disclosure under this subsection shall be subject to the same prohibition of disclosure.
- (e) IMMUNITY FROM CIVIL LIABILITY— Any person, including officers, agents, and employees, who in good faith produce the records or items requested in a subpoena shall not be liable in any court of any State or the United States to any customer or other person for such production or for non-disclosure of that production to the customer or other person, in compliance with the terms of a court order for non-disclosure.”
“Sec. 2332j. Administrative subpoenas in terrorism investigations”.

SECTION 154. STRENGTHENING ACCESS TO AND USE OF INFORMATION IN NATIONAL SECURITY INVESTIGATIONS.

- (a) VIOLATION OF NONDISCLOSURE PROVISIONS FOR NATIONAL SECURITY LETTERS AND COURT ORDERS.—Section 1510(e) of title 18, United States Code, is amended by striking the existing provision and replacing with:
“(e) Whoever violates section 2709(c) or 2332f(d) of this title, section 625(d) or 626(c) of the Fair Credit Reporting Act, section 1114(a)(3) or (5)(D) of the Right to Financial Privacy Act, section 802(b) of the National Security Act of 1947, or section 501(d) of the Foreign Intelligence Surveillance Act of 1978, shall be imprisoned for not more than seven days, and if the violation is committed with the intent to obstruct an investigation or judicial proceeding, shall be imprisoned for not more than 14 days.”
- (b) JUDICIAL ENFORCEMENT OF NATIONAL SECURITY LETTERS—Chapter 113B of title 18, United States Code, is amended by inserting before section 2333 the following:
“Sec. 2332k. Enforcement of requests for information.
In the case of a refusal to comply with a request for records, a report, or other information made to any person under section 2709(b) of this title,

section 625(a) or (b) or 626(a) of the Fair Credit Reporting Act, section 114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General may invoke the aid of any court of the United States with whose jurisdiction the investigation is carried on or the person resides, carries on business, or may be found, to compel compliance with the request. The court may issue an order requiring the person to comply with the request. Any failure to obey the order of the court may be punished by the court as contempt thereof. Any process under this section may be served in any judicial district in which the person may be found.”

TITLE II—PROTECTING NATIONAL SECURITY INFORMATION

Subtitle A—Safeguarding Classified Information

SECTION 201. DEFINITIONS.

For purposes of this Title:

- (a) “Access” means the ability or opportunity to gain knowledge of classified information.
- (b) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.
- (c) “Classified national security information” or “classified information” means information that has been determined pursuant to this Title or any executive order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
- (d) “Foreign government information” means:
 - (i) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; or
 - (ii) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence;

SECTION 202. CLASSIFICATION STANDARDS.

- (a) Information may be originally classified under this Title only if all of the following conditions are met:
 - (i) an original classification authority is classifying the information;
 - (ii) the information is owned by, produced by or for, or is under the control of the United States Government;
 - (iii) the information falls within one or more of the categories of information listed in section 105 of this Act; and
 - (iv) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.
- (b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not amplify or modify the substantive criteria or procedures for classification; or create any substantive or procedural rights subject to judicial review.
- (c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.
- (d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

SECTION 203. CLASSIFICATION LEVELS.

- (a) Information may be classified at one of the following three levels:
 - (i) “Top Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
 - (ii) “Secret” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
 - (iii) “Confidential” shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
- (b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

- (c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

SECTION 204. CLASSIFICATION AUTHORITY.

- (a) The authority to classify information originally may be exercised only by:
 - (i) the President and the Vice President;
 - (ii) agency heads and officials designated within this Title or otherwise by the President; and
 - (iii) United States Government officials delegated this authority pursuant to paragraph (c) of this section.
- (b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

- (i) Delegations of original classification authority shall be limited to the minimum required to administer this Title. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.
- (ii) “Top Secret” original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(ii) of this section.
- (iii) “Secret” or “Confidential” original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(ii) of this section, or the senior agency official designated under **section 5.4(d)** of this order, provided that official has been delegated “Top Secret” original classification authority by the agency head.
- (iv) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.
- (v) Delegations of original classification authority shall be reported or made available by name or position to the Director of National Intelligence.

(d) General classification authority.

- (i) Consistent with paragraph (a)(ii)—
 - (1) “Top Secret” original classification authority shall be exercised by the—
 - a) Assistant to the President and Chief of Staff
 - b) Assistant to the President for National Security Affairs
 - c) Assistant to the President for Homeland Security Affairs
 - d) Secretary of State

- e) Secretary of the Treasury
 - f) Secretary of Defense
 - g) Attorney General
 - h) Secretary of Homeland Security
 - i) Director of National Intelligence
 - j) Secretary of the Army
 - k) Secretary of the Navy
 - l) Secretary of the Air Force
 - m) Director of the Central Intelligence Agency
- (2) “Secret” original classification authority shall be exercised by the—
- a) Secretary of Commerce

SECTION 205. CLASSIFICATION CATEGORIES.

Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 203 of this Title, and it pertains to one or more of the following:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- (h) the development, production, or use of weapons of mass destruction.

SECTION 206. DURATION OF CLASSIFICATION.

- (a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts

of weapons of mass destruction, the date or event shall not exceed the time frame established by paragraph (b) of this section.

- (b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification six months from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to one year from the date of the original decision.
 - (i) The Director of National Intelligence may, upon notification to the congressional intelligence committees, provide guidance for the classification of information beyond one year.
- (c) No information may remain classified indefinitely.

SECTION 207. IDENTIFICATION AND MARKINGS.

- (a) All classified information shall retain banner and portion markings designating such document or portion as classified.
- (b) The Director of National Intelligence shall provide further guidance on the identification and marking of classified information.
- (c) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

SECTION 208. CLASSIFICATION PROHIBITIONS AND LIMITATIONS.

- (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:
 - (i) conceal violations of law, inefficiency, or administrative error;
 - (ii) prevent embarrassment to a person, organization, or agency;
 - (iii) restrain competition; or
 - (iv) prevent or delay the release of information that does not require protection in the interest of the national security.
- (b) Information may not be reclassified after declassification and release to the public under proper authority unless approved by the President in consultation with the Assistant to the President for National Security Affairs, the Director of National Intelligence, and the Attorney General.
- (c) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:
 - (i) meets the standards for classification under this order; and
 - (ii) is not otherwise revealed in the individual items of information.

SECTION 209. ACTION BY ATTORNEY GENERAL.

- (a) ***Criminal Penalty.*** Whoever, knowingly, willfully, or negligently engages in the prohibited conduct of paragraph (a) of section 208 of this Title shall be fined under this Title, and be imprisoned not more than ten days.
- (b) ***Declassification Authority.*** If the Attorney General determines that information is classified in violation of this Title, the Attorney General may require the information to be declassified by the agency that originated the classification. Any such decision by the Attorney General may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(c) Sanctions.

- (i) If the Attorney General finds that a violation of this Title or its implementing directives has occurred, the Attorney General shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.
- (ii) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:
 - (1) disclose to unauthorized persons information properly classified under this order or predecessor orders;
 - (2) classify or continue the classification of information in violation of this order or any implementing directive;
 - (3) create or continue a special access program contrary to the requirements of this order; or
 - (4) contravene any other provision of this order or its implementing directives.
- (iii) Sanctions may include reprimand, suspension, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.
- (iv) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this Title.
- (v) ***Reporting Requirements.*** The agency head or senior agency official shall:
 - (1) take appropriate and prompt corrective action when a violation or infraction under subparagraph (ii) of this section occurs; and
 - (2) notify the Attorney General when a violation under paragraph (ii)(1), (2), or (3) of this section occurs.

SECTION 210. CLASSIFICATION CHALLENGES.

Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with procedures established by the Director of National Intelligence.

SECTION 211. DERIVATIVE CLASSIFICATION.

- (a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.
- (b) Persons who apply derivative classification markings shall mark all identifications and markings consistent with section 207 of this Title.
- (c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

SECTION 212. CLASSIFICATION GUIDES.

Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this Title.

SECTION 213. DECLASSIFICATION AND DOWNGRADING.

- (a) Information shall be declassified as soon as it no longer meets the standards for classification under this Title.
- (b) Information shall be declassified or downgraded by:
 - (i) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;
 - (ii) the originator's current successor in function, if that individual has original classification authority;
 - (iii) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or
 - (iv) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.
- (c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify,

downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

- (d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure.
- (e) ***Exemption from Automatic Declassification.*** Except as otherwise provided, an agency head may exempt from automatic declassification specific information, the release of which should clearly and demonstrably be expected to:
- (i) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;
 - (ii) reveal information that would assist in the development, production, or use of weapons of mass destruction;
 - (iii) reveal information that would impair U.S. cryptologic systems or activities;
 - (iv) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;
 - (v) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;
 - (vi) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;
 - (vii) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;
 - (viii) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

- (ix) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at one year.

SECTION 213. SAFEGUARDING INFORMATION.

- (a) A person may have access to classified information provided that:
 - (i) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
 - (ii) the person has signed an approved nondisclosure agreement; and
 - (iii) the person has a need-to-know the information.
- (b) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.
- (c) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.
- (d) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.
- (e) ***Emergency Distribution.*** In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

SECTION 214. SPECIAL ACCESS PROGRAMS.

- (a) ***Establishment of special access programs.*** Unless otherwise authorized by the President, only the Secretaries of State, Defense, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:
 - (i) the vulnerability of, or threat to, specific information is exceptional; and

- (ii) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.
- (b) ***Requirements and limitations.***
 - (i) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.
 - (ii) Upon request, an agency head shall brief the Assistant to the President for National Security Affairs, or a designee, on any or all of the agency's special access programs.
- (c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Subtitle B—Protected Information Otherwise

SECTION 230. PROHIBITION OF DISCLOSURE OF TERRORISM INVESTIGATION DETAINEE INFORMATION.

Notwithstanding section 552 of title 5, United States Code, or any other provision of law, no officer, employee, or agency of the United States shall disclose, without the prior determination of the Attorney General and the Director of the Central Intelligence Agency that such disclosure would not adversely impact the national security interests of the United States, the names or other identifying information relating to any alien who is detained within the United States, or any individual who is detained outside the United States, in the course of any investigation of international terrorism until such time as such individual is served with a criminal information.

SECTION 231. INFORMATION RELATING TO CAPITOL BUILDINGS.

Notwithstanding section 552 of title 5, United States Code, or any provision of law, information within the possess of any officer, employee or agency of the Executive branch of government relating to the United States Capitol and relating buildings, shall not be disclosed under section 552(a) of title 5 United States Code, by such Executive Branch officer, employee or agency.

SECTION 232. EX PARTE AUTHORIZATIONS UNDER CLASSIFIED INFORMATION PROCEDURES ACT.

Section 4 of the Classified Information Procedures Act (18 U.S.C. App. 3) is hereby amended by deleting the "may" in the second sentence and inserting "shall".

TITLE III—ENHANCING INVESTIGATIONS OF TERRORIST PLOTS

Subtitle A—Facilitating Information Sharing and Cooperation

SECTION 301. SHORT TITLE.

This Subtitle may be cited as the "Information Sharing and Cooperation Act of 2022"

SECTION 302. APPROPRIATE REMEDIES WITH RESPECT TO LAW ENFORCEMENT SURVEILLANCE ACTIVITIES.

(a) Requirements for relief—

(i) Prospective relief—

- (1)** Prospective relief in any civil action with respect to law enforcement surveillance activities shall extend no further than necessary to correct the current and ongoing violation of the Federal right of a particular plaintiff or plaintiffs. The court shall not grant or approve any prospective relief unless the court finds that such relief is narrowly drawn, extends no further than necessary to correct the violation of the Federal right, and is the least intrusive means necessary to correct the violation of the Federal right. The court shall give substantial weight to any adverse impact on national security, public safety, or the operation of a criminal justice system caused by the relief.
- (2)** The court shall not order any prospective relief that requires a government official to refrain from exercising his authority under applicable law, unless—
 - a)** Federal law requires such relief be ordered;
 - b)** the relief is necessary to correct the violation of a Federal right; and
 - c)** no other relief will correct the violation of the Federal right.
- (3)** Nothing in this section shall be construed to authorize the courts, in exercising their remedial powers, to repeal or detract from otherwise applicable limitations on the remedial powers of the courts.

- ##### **(ii) Preliminary injunctive relief—**
- In any civil action with respect to law enforcement surveillance activities, to the extent otherwise authorized by law, the court may enter a temporary restraining order or an order for

preliminary injunctive relief. Preliminary injunctive relief must be narrowly drawn, extend no further than necessary to correct the harm the court finds requires preliminary relief, and be the least intrusive means necessary to correct that harm. The court shall give substantial weight to any adverse impact on public safety or the operation of a criminal justice system caused by the preliminary relief and shall respect the principles of comity set out in paragraph (i)(2) in tailoring any preliminary relief. Preliminary injunctive relief shall automatically expire on the date that is ten days after its entry, unless the court makes the findings required under subsection (a)(i) for the entry of prospective relief and makes the order final before the expiration of the ten-day period.

(b) Termination of relief—

(i) Termination of prospective relief—

(1) In any civil action with respect to law enforcement surveillance activities in which prospective relief is ordered, such relief shall be terminable upon the motion of any party or intervener—

- a) ten days after the date the court granted or approved the prospective relief,
- b) five days after the date the court has entered an order denying termination of prospective relief under this paragraph; or

(2) Nothing in this section shall prevent the parties from agreeing to terminate or modify relief before the relief is terminated under subparagraph (1)

(ii) Immediate termination of prospective relief— In any civil action with respect to law enforcement surveillance activities, a defendant or intervener shall be entitled to the immediate termination of any prospective relief if the relief was approved or granted in the absence of a finding by the court that the relief is narrowly drawn, extends no further than necessary to correct a current and ongoing violation of the Federal right, and is the least intrusive means necessary to correct the violation of the Federal right.

(iii) Limitation— Prospective relief shall not terminate if the court makes written findings based on the record that prospective relief remains necessary to correct a current and ongoing violation of the Federal right, extends no further than necessary to correct the violation of the Federal right, and that the prospective relief is narrowly drawn and the least intrusive means to correct the violation.

- (iv) Termination or modification of relief— Nothing in this section shall prevent any party or intervener from seeking modification or termination before the relief is terminable under paragraph (i) or (ii), to the extent that modification or termination would otherwise be legally permissible.
- (v) Settlements—
 - (1) Consent decrees— In any civil action with respect to law enforcement surveillance activities, the court shall not enter or approve a consent decree unless it complies with the limitations set forth in subsection (a)

SECTION 303. DISCLOSURE OF INFORMATION.

Notwithstanding any other law, a commercial or business entity, and any employee or agent of such a commercial or business entity, shall not be subject to civil liability in any court for the voluntary provision or disclosure of information to a Federal law enforcement agency, based on a reasonable belief that the information may assist in the investigation or prevention of terrorist activities (as defined in section 2510 of title 18, United States Code).

TITLE IV—ENHANCING PROSECUTION AND PREVENTION OF TERRORIST CRIMES

Subtitle A—Increased Penalties and Protections Against Terrorist Acts

SECTION 401. SHORT TITLE.

This title may be cited as the "Protecting Against Terrorism Act of 2022"

SECTION 402. TERRORISM HOAXES.

PROHIBITION ON HOAXES— Chapter 47 of title 18, United States Code, is amended by inserting after section 1040 the following:

“Sec. 1041. False information and hoaxes

- (a) CRIMINAL VIOLATION— Whoever engages in any conduct, with intent to convey false or misleading information, under circumstances where such information may reasonably be believed and where such information concerns an activity which would constitute a violation of section 175, 229, 831, or 2332a, shall be fined under this title and imprisoned not more than five days, or both.”

SECTION 403. PROVIDING MATERIAL SUPPORT TO TERRORISM.

- (a) Section 2339A(a) of title 18, United States Code, is amended by—
- (i) designating the first sentence as paragraph (1)
 - (ii) designating the second sentence as paragraph (3)
 - (iii) inserting after “for life.” the following:

“(2) Whoever, in or affecting interstate or foreign commerce, or while outside the United States and a national of the United States (as defined in section 1203(c)) or a legal entity organized under the laws of the United States (including of any of its States, districts, commonwealth, territories, or possessions), provides material support or resources or conceals or disguises the nature, location, source or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, an act of international or domestic terrorism (as defined in section 2331), or in the preparation for, or in carrying out, the concealment or escape from the commission of such act, or attempts or conspires to do so, shall be punished as provided under paragraph (1).”; and
 - (iv) by inserting “act” after “underlying”.
- (b) Section 2331(1)(B) and (5)(B) of title 18, United States Code, are each amended by inserting "by their nature or context" after "appear".
- (c) Section 2339A(b) of title 18, United States Code, is amended by adding at the end of the following: "The term 'training' means instruction or teaching designed to impart a specific skill."
- (d) Section 2339B(g)(4) of title 18, United States Code, is amended to read as follows:
- “(4) the term 'material support or resources' has the same meaning as in section 2339A (including the definition of 'training' in that section), except that no person may be prosecuted under this section in connection with the term 'personnel' unless that person has knowingly provided, attempted to provide, or conspired to provide a terrorist organization with one or more individuals (which may be or include himself) to work in concert with the organization or under its direction or control;”.

SECTION 404. USE OF ENCRYPTION TO CONCEAL CRIMINAL ACTIVITY.

Part I of title 18, United States Code, is amended by inserting after chapter 123 the following:

"CHAPTER 124 — ENCRYPTED WIRE OR ELECTRONIC
COMMUNICATIONS AND STORED ELECTRONIC INFORMATION

Sec. 2801. Unlawful use of encryption.

- (a) Any person who, during the commission of a felony under Federal law, knowingly and willfully encrypts any incriminating communication or information relating to that felony—
 - (i) in the case of a first offense under this section, shall be imprisoned not more than seven days, fined under this title, or both; and
 - (ii) in the case of a second or subsequent offense under this section, shall be imprisoned not more than 14 days, fined under this title, or both.
- (b) The terms 'encrypt' and 'encryption' refer to the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information."

SECTION 405. PRESUMPTION FOR PRETRIAL DETENTION IN CASES INVOLVING TERRORISM.

Section 3142 of title 18, United States Code, is amended—

- (1) in subsections (e) —
 - (a) by inserting “or” before “the Maritime”; and
 - (b) by striking ", or an offense under section 924(c), 956(a), or 2332b of title 18 of the United States Code" and inserting ", an offense under section 924(c), or an offense described in section 2332b(g)(5)(B)"; and
- (2) in subsections (f)(1)(A) and (g)(1), by inserting "or an offense described in section 2332b(g)(5)(B)" after "violence".

SECTION 406. POST-RELEASE SUPERVISION OF TERRORISTS.

Section 3583 of title 18, United States Code, is amended—

- (1) in subsection (e)(3), by inserting "on any such revocation" after "required to serve";
- (2) in subsection (h), by striking "that is less than the maximum term of imprisonment authorized under subsection (e)(3)"; and
- (3) in subsection (j)—

- (a) by striking ", the commission" and all that follows through "person,"; and
- (b) by inserting "and the sentence for any such offense shall include a term of supervised release of at least 14 days" before the period.

SECTION 407. SUSPENSION, REVOCATION, AND DENIAL OF CERTIFICATES FOR BUSINESSES FOR NATIONAL SECURITY REASONS.

(a) Suspension of Certificate—

- (i) ***Notification of Initial Threat Determination***— The Under Secretary of Commerce for Industry and Security or designee shall notify the Chairman of the Licensing Board of the identity of—

- (1) any holder of a certificate issued by the Licensing Board on whom the Under Secretary or designee has served an initial determination that the certificate holder poses a threat to economic security or national security; or
- (2) any holder of a certificate issued by the Licensing Board on whom the Under Secretary or designee has served an initial determination that the individual who has a controlling or ownership interest in the certificate holder poses a threat to economic security or national security by virtue of that interest.

- (ii) ***Suspension***— The Chairman of the Licensing Board shall issue an order suspending any certificate identified by the Under Secretary or designee pursuant to paragraph (i)(1) or (2). The Chairman's order of suspension shall be immediately effective and remain effective until—

- (1) the Chairman withdraws the order; or
- (2) the Chairman issues an order revoking the certificate or special permit.

The Chairman's order of suspension is not subject to administrative or judicial review.

- (iii) ***Opportunity to Respond to Initial Threat determination***— The Under Secretary or designee shall afford certificate holders and persons with a controlling or ownership interest identified in paragraph (i)(1) or (2) notice and an opportunity to respond to an initial determination that the certificate holders or persons pose a threat to economic security or national security prior to the issuance of a final threat determination.
- (iv) ***Judicial Review of Initial Threat Determination***— The initial determination by the Under Secretary or designee that a certificate holder or person with a controlling or ownership interest identified in subsection

(a)(i)(1) or (2) poses a threat to economic security or national security is not subject to judicial review.

(b) Revocation of Certificate—

(i) ***Notification of Final Threat Assessment***— The Under Secretary or designee shall notify the Chairman of the identity of any certificate holder described in subsection (a)(i)(1) or (2) on whom—

(1) a withdrawal of initial threat determination has been served; or

(2) a final threat determination has been served.

The Under Secretary or designee must issue either a withdrawal of final determination within five days of the notification of initial threat determination.

(ii) ***Revocation***— The Chairman shall issue an order revoking the certificate held by a certificate holder described in subsection (a)(i)(1) or (2) on whom the Under Secretary or designee has served a final determination that the certificate holder poses a threat to economic security or national security or that a person who has a controlling or ownership interest in the certificate holder poses a threat to economic security or national security by virtue of that interest. The Chairman's order of revocation shall be immediately effective.

(iii) ***Review of Final Threat Determination and Order of Revocation***—

(1) A final threat determination by the Under Secretary or designee or an order of revocation issued by the Chairman with regard to a person who is neither a citizen nor permanent resident alien of the United States is not subject to administrative or judicial review.

(2) A person who is a citizen or permanent resident alien of the United States disclosing a substantial interest in a final threat determination by the Under Secretary or designee under paragraph (i) and an order of revocation issued by the Administrator under paragraph (ii) may seek review of those actions by filing a petition for review in the United States District Court for the District of Columbia. The petition for review must be filed not later than three days after the issuance of the order of revocation. The court may allow the petition to be filed after the third day only if there are reasonable grounds for not filing by the third day. The court's review is limited to determining whether it was arbitrary, capricious, or otherwise not according to law for the Under Secretary to make the final threat determination and for the Chairman to issue the order of revocation.

- (3) In any judicial review of the Under Secretary's determination and the Chairman's order under paragraphs (i) and (ii), if the actions were based on classified information (as defined in section 1(a) of the Classified Information Procedures Act) or sensitive security information (as defined in regulations issued under section 40119(b) of this title) such information may be submitted to the reviewing court *ex parte* and *in camera*.

(c) Denial of Certificate—

- (i) ***Notification of Threat Determination***— The Under Secretary or designee shall notify the Chairman of the identity of—
- (1) any person on whom the Under Secretary or designee has served an initial or final determination that the person poses a threat to economic security or national security; or
 - (2) the entity on whom the Under Secretary or designee has served an initial or final determination that a person who has a controlling or ownership interest in the entity poses a threat to economic security or national security by virtue of that interest.
- (ii) ***Denial***— The Chairman may not issue a certificate to any person or entity identified in paragraph (i) unless the Under Secretary or designee has withdrawn a determination that the person poses a threat. A denial of certificate based on an initial threat determination is not subject to administrative or judicial review.
- (iii) ***Opportunity to Respond to Initial Threat determination***— The Under Secretary or designee shall afford applicants for certificates and persons with a controlling or ownership interest identified in paragraph (i)(1) or (2) notice and an opportunity to respond to an initial determination that an applicant for a certificate or person with a controlling or ownership interest in an applicant poses a threat to economic security or national security prior to the final determination of threat assessment.
- (iv) ***Review of Initial Threat Determination***— The initial determination by the Under Secretary or designee that an applicant for a certificate or person with a controlling ownership interest in an applicant poses a threat to civil aviation or national security is not subject to judicial review.
- (v) ***Review of Final Threat Determination and Certificate Denial***—
- (1) A final threat determination by the Under Secretary or designee and the denial of certificate by the Chairman under this subsection with regard to a person who is not a citizen or resident alien of the United States is not subject to administrative or judicial review.

- (2) A citizen or permanent resident alien of the United States may seek review of a final threat determination by the Under Secretary or designee and denial by the Chairman under this subsection by filing a petition for review in the United States District Court for the District of Columbia. The petition must be filed no later than the third day after the issuance of the denial. The court may allow the petition to be filed after the third day only if there are reasonable grounds for not filing by the third day. The court's review is limited to determining whether it was arbitrary, capricious, or otherwise not according to law for the Under Secretary to make the final threat determination and for the Chairman to deny a certificate.
- (3) In any judicial review of the Under Secretary's final threat determination and the Chairman's denial, if the actions were based on classified information (as defined in section 1(a) of the Classified Information Procedures Act) or sensitive security information (as defined in regulations issued under section 40119(b) of this title) such information may be submitted to the reviewing court *ex parte* and *in camera*.
- (d) Coordination with the Attorney General— Nothing in this section is intended to alter any provisions of law. The Under Secretary shall coordinate any request to the Chairman of the Licensing Board under this section with the Attorney General on matters within the Attorney General's jurisdiction.
- (e) As used in this section, “certificate” means any license, special permit, or status issued by the Department of Commerce’s Licensing Board for the purposes of enabling a commercial activity.

SECTION 408. NO STATUTE OF LIMITATIONS FOR TERRORISM CRIMES.

- (a) Section 3286(b) of title 18, United States Code, is amended by striking ", if the commission" and all that follows through "person".
- (b) This section shall supersede any conflicting provision within the Criminal Statute of Limitations Act.

SECTION 409. PENALTIES FOR TERRORIST MURDERERS.

Chapter 113B title 18, United States Code, is amended, by inserting—
“2339E. Terrorist offenses resulting in death.

A person who, in the course of an offense listed in section 2332b(g)(5)(B) or of terrorist activities (as defined in section 2510), engages in conduct

that results in the death of a person, shall be punished by imprisonment for any term of days, but no less than fourteen days.”

(b) Section 3592(c)(1) of title 18, United States Code, is amended by inserting "section 2339E (terrorist offenses resulting in death)," after "destruction),"

Subtitle B—Incapacitating Terrorist Financing

SECTION 420. CORRECTIONS OF FINANCING OF TERRORISM STATUTE.

(a) Section 2339C(c)(2) of title 18, United States Code, is amended by—

- (i) striking "resources, or funds" and inserting "resources, or any funds or proceeds of such funds";
- (ii) in subparagraph (A), striking "were provided" and inserting "are to be provided, or knowing that the support or resources were provided,"; and
- (iii) in subparagraph (B)—
 - (1) striking "or any proceeds of such funds"; and
 - (2) striking "were provided or collected" and inserting "are to be provided or collected, or knowing that the funds were provided or collected,"
- (iv) Section 2339C(e) is amended by—
 - (1) striking "and" at the end of paragraph (12);
 - (2) redesignating paragraph (13) as paragraph (14); and
 - (3) inserting after paragraph (12) the following new paragraph:

"(13) the term 'material support or resources' has the same meaning as in section 2339A(b) of this title; and".

GROUP B—COMBATTING ORGANIZED CRIME

TITLE V—STRENGTHENING CRIMINAL INTELLIGENCE

SECTION 501. DEFINITIONS.

In this Title—

- (a) “criminal intelligence” means information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.
- (b) “strategic intelligence” means information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short- and long-term investigative goals.

- (c) “tactical intelligence” means information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations and provide for officer safety.
- (d) “threshold for criminal intelligence” means the threshold for collecting information and producing criminal intelligence shall be the "reasonable suspicion" standard.
- (e) “reasonable suspicion” or *Criminal Predicate* is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.
- (f) “OIC” means the designated officer or official in charge.

SECTION 502. CRIMINAL INTELLIGENCE PLAN

- (a) The Attorney General shall develop a comprehensive national criminal intelligence strategy to meet criminal intelligence objectives for the following two months, or a longer period, if appropriate.
- (b) Each national intelligence strategy required by subsection (a) shall—
 - (i) the strategic plans of other relevant departments and agencies of the United States; and
 - (ii) other relevant national-level plans;
 - (iii) address matters related to national, military, and local criminal intelligence;
 - (iv) identify the major criminal intelligence missions that the law enforcement community is currently pursuing and will pursue in the future to meet the anticipated security environment;
 - (v) describe how the law enforcement community will utilize personnel, technology, partnerships, and other capabilities to pursue the major criminal intelligence missions identified in paragraph (iv);
 - (vi) other information the Attorney General may deem necessary.
- (c) ***Submission to Congress.*** The Attorney General shall submit to the congressional judiciary committees a report on each national criminal intelligence strategy required by subsection (a) not later than seven days after the date of the completion of such strategy.

SECTION 503. CRIMINAL INTELLIGENCE COORDINATION COUNCIL.

- (a) There is a Criminal Intelligence Coordination Council.
- (b) ***Membership.*** The Criminal Intelligence Coordination Council shall consist of the following:
 - (i) The Attorney General, or his designee, who shall chair the Council.

- (ii) The Executive Assistant Director of the Federal Bureau of Investigation for the Criminal, Cyber, Response, and Services Branch, or successor position, or other official designated by the Attorney General.
 - (iii) The Assistant Director of Strategic Intelligence of the Bureau of Alcohol, Tobacco, Firearms or Explosives, or a successor position;
 - (iv) The Under Secretary of Homeland Security for Intelligence and Analysis;
 - (v) The Assistant Director of the United States Secret Service for Strategic Intelligence or successor position;
 - (vi) The Assistant Director United States Marshal Service for the Criminal Intelligence Branch or successor position;
 - (vii) a Representative, designated by the Director of National Intelligence, from the Office of the Director of National Intelligence, with principal responsibility for the Director of National Intelligence's partner engagement and information-sharing programs.
 - (viii) The Chief of the Metropolitan Police Department's senior official responsible for criminal intelligence unit; and
 - (ix) Such other officers of the United States and District of Columbia Governments as the Attorney General may designate from time to time.
- (c) **Functions.** The Criminal Intelligence Coordination Council shall assist the Attorney General in developing and implementing a joint, unified criminal intelligence effort to combat major and violent crimes by—
- (i) advising the Attorney General on establishing requirements, and monitoring and evaluating the performance of the criminal intelligence community, and on such other matters as the Attorney General may request; and
 - (ii) ensuring the timely execution of programs, policies, and directives established or developed by the Attorney General.
- (d) **Meetings.** The Attorney General shall convene meetings of the Criminal Intelligence Coordination Council as the Attorney General considers appropriate.

SECTION 504. PROTECTING CRIMINAL INTELLIGENCE.

- (a) **Authority of the Attorney General.** The Attorney General shall develop guidelines to safeguard the security of criminal intelligence, including classified criminal intelligence information, which shall not be construed to mean classified national security information, as established under Group A of this Act, which remains under the jurisdiction of the Director of National Intelligence.
- (b) **Classification of Intelligence.** Criminal Intelligence files may be classified in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable this agency to control access to intelligence. These

classifications shall be reevaluated whenever new information is added to an existing intelligence file.

- (i) ***Restricted.*** "Restricted" intelligence files include those that contain information that could adversely affect an ongoing investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the intelligence OIC or the agency chief executive to authorized law enforcement agencies with a need and a right to know.
 - (ii) ***Confidential.*** "Confidential" intelligence is less sensitive than restricted intelligence. It may be released to agency personnel when a need and a right to know has been established by the intelligence OIC or his designate.
 - (iii) ***Unclassified.*** "Unclassified" intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to officers conducting authorized investigations that necessitate this information.
- (c) ***Security of Intelligence.*** All restricted and confidential files shall be secured, and access to all intelligence information shall be controlled and recorded by procedures established by the intelligence OIC.
- (i) Informant files shall be maintained separately from intelligence files.
 - (ii) Intelligence files shall be maintained in accordance with Attorney General Guidelines, applicable federal law, and in the case of the Metropolitan Police Department, local law.
 - (iii) Release of intelligence information in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency shall be made only with the express approval of the intelligence OIC and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of this agency's OIC.
 - (iv) All files released under freedom of information provisions or through disclosure shall be carefully reviewed.
- (d) ***Auditing and Purging Files.***
- (i) The OIC is responsible for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. To that end, all intelligence files shall be audited and purged on an annual basis as established by the agency OIC through an independent auditor.
 - (ii) When a file has no further information value and/or meets the criteria of any applicable law, it shall be destroyed. A record of purged files shall be maintained by the intelligence authority

TITLE VI—ADAPTING TO RACKETEERING INFLUENCED AND CORRUPT ORGANIZATIONS

SECTION 601. SHORT TITLE; AMENDMENTS.

This title may be cited as the “Racketeering Influenced and Corrupt Organizations Act of 2022” and shall supersede 18 U.S. Code Chapter 96.

SECTION 602. DEFINITIONS.

In this Title—

- (a) “racketeering activity” means
 - (i) any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled firearm under the laws of the District of Columbia.
 - (ii) any act which is indictable under any of the provisions of title 18, United States Code, including acts of terrorism.
- (b) “enterprise” includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity;
- (c) “pattern of racketeering activity” requires at least two acts of racketeering activity;
- (d) “racketeering investigator” means any attorney or investigator so designated by the Attorney General and charged with the duty of enforcing or carrying into effect this chapter;
- (e) “racketeering investigation” means any inquiry conducted by any racketeering investigator for the purpose of ascertaining whether any person has been involved in any violation of this chapter or of any final order, judgment, or decree of any court of the United States, duly entered in any case or proceeding arising under this chapter;
- (f) “documentary material” includes any book, paper, document, record, recording, or other material; and
- (g) “Attorney General” includes the Attorney General of the United States, the Deputy Attorney General of the United States, the Associate Attorney General of the United States, any Assistant Attorney General of the United States, or any employee of the Department of Justice or any employee of any department or agency of the United States so designated by the Attorney General to carry out the powers conferred on the Attorney General by this chapter. Any department or agency so designated may use in investigations authorized by this chapter either the investigative provisions of this chapter or the investigative power of such department or agency otherwise conferred by law.

SECTION 603. PROHIBITED ACTIVITIES.

- (a) It shall be unlawful for any person to directly or indirectly engage in, or actually or intends to, profit from a pattern of racketeering activity within the meaning of section 602 of this Title, engage or otherwise participate in, further advancement of interests, in acquisition of any interest in, or the establishment or operation of, any enterprise which is engaged in, or the activities of which (1) affect interstate or foreign commerce (2) disturb the peace or good conduct of government (3) hinder, obstruct, or otherwise deny the exercise of rights guaranteed by the Constitution of the United States.
- (b) It shall be unlawful for any person through a pattern of racketeering activity to acquire or maintain, directly or indirectly, any interest in or control of any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.
- (c) It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity.
- (d) It shall be unlawful for any person to conspire to violate any of the provisions of subsection (a), (b), or (c) of this section.

SECTION 604. CRIMINAL PENALTIES.

- (a) Whoever violates any provision of section 603 of this title shall be fined under this title or imprisoned not more than fourteen days (or no less if the violation is based on a racketeering activity for which the maximum penalty includes life imprisonment or a penalty for fourteen days), or both, and shall forfeit to the United States, irrespective of any provision of State law—
 - (i) any interest the person has acquired or maintained in violation of section 603;
 - (ii) any—
 - (1) interest in;
 - (2) claim against; or
 - (3) property or contractual right of any kind affording a source of influence over;

any enterprise which the person has established, operated, controlled, conducted, or participated in the conduct of, in violation of section 603;
and
 - (iii) any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from racketeering activity in violation of section 603.

The court, in imposing sentence on such person shall order, in addition to any other sentence imposed pursuant to this section, that the person forfeit to the United States all property described in this section. In lieu of a fine otherwise authorized by this section, a defendant who derives profits or other proceeds from an offense may be fined not more than twice the gross profits or other proceeds.

(b) Property subject to criminal forfeiture under this section includes—

- (i) real property, including things growing on, affixed to, and found in land; and
- (ii) tangible and intangible personal property, including rights, privileges, interests, claims, and securities.

(c) A temporary restraining order may be entered upon application of the United States without notice or opportunity for a hearing when an information has not yet been filed with respect to the property, if the United States demonstrates that there is probable cause to believe that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section and that provision of notice will jeopardize the availability of the property for forfeiture.

SECTION 605. CIVIL REMEDIES.

(a) Actions by the Court.

- (i) The district courts of the United States shall have jurisdiction to prevent and restrain violations of section 2003 of this Title by issuing appropriate orders, including, but not limited to: ordering any person to divest himself of any interest, direct or indirect, in any enterprise; imposing reasonable restrictions on the future activities or investments of any person, including, but not limited to, prohibiting any person from engaging in the same type of endeavor as the enterprise engaged in, the activities of which affect interstate or foreign commerce; or ordering dissolution or reorganization of any enterprise, making due provision for the rights of innocent persons.
- (ii) The Attorney General may institute proceedings under this subsection (a). Pending final determination thereof, the court may at any time enter such restraining orders or prohibitions, or take such other actions, including the acceptance of satisfactory performance bonds, as it shall deem proper.
- (iii) Any person injured in his business or property by reason of a violation of section 2003 of this Title may sue therefore in any appropriate United States district court and shall recover threefold the damages he sustains, except that no person may rely upon any conduct that would have been actionable as fraud. The exception contained in the preceding sentence does not apply to an action against any person that is criminally convicted in connection with the fraud.

- (iv) A final judgment or decree rendered in favor of the United States in any criminal proceeding brought by the United States under this chapter shall estop the defendant from denying the essential allegations of the criminal offense in any subsequent civil proceeding brought by the United States.

(b) Actions by the Attorney General.

- (i) The Attorney General shall have the authority to designate enterprises engaged in a pattern of racketeering as a criminal enterprise. Such designation shall be made publicly. The authorities and responsibilities set forth in this section are not subject to judicial review.
- (ii) Designations of a criminal enterprise under this Title shall—
 - (1) prohibit any member of such enterprise from being granted any additional licenses or special permits by the Department of Commerce or business authority of the District of Columbia;
 - (2) prohibit any member of such enterprise from accepting or holding a position in the Government of the United States or the government of the District of Columbia.
 - (3) prohibit any member of such enterprise from accepting or holding a firearms license or special permit by the Attorney General or the government of the District of Columbia.
- (iii) **Certifications of the Attorney General.** The Attorney General may certify any person previously associated with or otherwise separated from the criminal enterprise has not engaged in a pattern of racketeering activity and the Attorney General may waive the prohibitions under paragraph (ii) of this subsection (b).
- (iv) **Notifications of the Attorney General to Congress.** The Attorney General shall report to the judiciary committees of Congress any Officer of the United States, elected or appointed by the President, who is ineligible to hold office under subsection (b)(ii)(2) of this Title.

SECTION 606. VENUE AND PROCESS.

Any civil action or proceeding under this Title against any person may be instituted in the district court of the United States for any district in which such person resides, is found, has an agent, or transacts his affairs.

SECTION 607. EXPEDITION OF ACTIONS.

In any civil action instituted under this chapter by the United States in any district court of the United States, the Attorney General may file with the clerk of such court a certificate stating that in his opinion the case is of general public importance. A copy of that certificate shall be furnished immediately by such clerk to the chief judge or in his absence to the presiding

district judge of the district in which such action is pending. Upon receipt of such copy, such judge shall designate immediately a judge of that district to hear and determine action.

SECTION 608. EVIDENCE.

In any proceeding ancillary to or in any civil action instituted by the United States under this chapter the proceedings may be open or closed to the public at the discretion of the court after consideration of the rights of affected persons.

SECTION 609. CIVIL INVESTIGATIVE DEMAND.

- (a) Whenever the Attorney General has reason to believe that any person or enterprise may be in possession, custody, or control of any documentary materials relevant to a racketeering investigation, he may, prior to the institution of a civil or criminal proceeding thereon, issue in writing, and cause to be served upon such person, a civil investigative demand requiring such person to produce such material for examination.
- (b) Each such demand shall—
 - (i) state the nature of the conduct constituting the alleged racketeering violation which is under investigation and the provision of law applicable thereto;
 - (ii) describe the class or classes of documentary material produced thereunder with such definiteness and certainty as to permit such material to be fairly identified;
 - (iii) state that the demand is returnable forthwith or prescribe a return date which will provide a reasonable period of time within which the material so demanded may be assembled and made available for inspection and copying or reproduction; and
 - (iv) identify the custodian to whom such material shall be made available.
- (c) No such demand shall—
 - (i) contain any requirement which would be held to be unreasonable if contained in a subpoena duces tecum issued by a court of the United States;
- (d) Service of any such demand or any petition filed under this section may be made upon a person by—
 - (i) delivering a duly executed copy thereof to any partner, executive officer, managing agent, or general agent thereof, or to any agent thereof authorized by appointment or by law to receive service of process on behalf of such person, or upon any individual person; or
 - (ii) delivering a duly executed copy thereof to the principal office or place of business of the person to be served;
- (e) An affirmation of service by the individual serving any such demand or petition setting forth the manner of such service shall be prima facie proof of such service.
- (f)
 - (i) The Attorney General shall designate a racketeering investigator to serve as racketeer document custodian, and such additional racketeering investigators as

he shall determine from time to time to be necessary to serve as deputies to such officer.

- (ii) Any person upon whom any demand issued under this section has been duly served shall make such material available for inspection and copying or reproduction to the custodian designated therein at the principal place of business of such person, or at such other place as such custodian and such person thereafter may agree and prescribe in writing or as the court may direct, pursuant to this section on the return date specified in such demand, or on such later date as such custodian may prescribe in writing. Such person may upon written agreement between such person and the custodian substitute for copies of all or any part of such material originals thereof.
 - (iii) While in the possession of the custodian, no material so produced shall be available for examination, without the consent of the person who produced such material, by any individual other than the Attorney General as defined in section 603 of this title. Under such reasonable terms and conditions as the Attorney General shall prescribe, documentary material while in the possession of the custodian may be available for examination by the person who produced such material or any duly authorized representatives of such person.
- (g) Whenever any person fails to comply with any civil investigative demand duly served upon him under this section or whenever satisfactory copying or reproduction of any such material cannot be done and such person refuses to surrender such material, the Attorney General may file, in the district court of the United States for any judicial district in which such person resides, is found, or transacts business, and serve upon such person a petition for an order of such court for the enforcement of this section.

TITLE VII—MISCELLANEOUS PROVISIONS

SECTION 701. DUTIES OF ARCHIVIST.

The Archivist of the United States shall publish and compile all affected sections of the United States Code as amended. The Archivist shall certify to the congressional judiciary committees upon the completion of such compiling.

SECTION 702. COMMISSION ON CAPITAL DISTRICT SECURITY.

- (a) **Review.** The Secretary of Homeland Security shall lead a review of the United States Government's contingency plans, standard operating procedures, and all other apparatus and resources apportioned or otherwise relating to civil disorder and other emergencies occurring within the District of Columbia.

- (b) *Review participants.*** The Secretary of Homeland Security shall be assisted by, and receive all pertinent information from, the Secretary of State, the Secretary of Defense, and the Attorney General.
- (c) *Report to Congress.*** The Secretary of Homeland Security shall compile his findings, conclusions, and any recommendations to the congressional committees on homeland security no later than fourteen days after the passage of this Act.

SECTION 703. ENACTMENT.

This Act shall go into effect immediately upon passage.