JIM JORDAN, Ohio
CHAIRMAN

JERROLD NADLER, New York
RANKING MEMBER

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–6906
judiciary.house.gov

May 28, 2024

The Honorable Merrick B. Garland
Attorney General
Department of Justice
Washington, DC 20530

Dear Attorney General Garland:

On April 20, 2024, President Biden signed into law H.R. 7888, the "Reforming Intelligence and Securing America Act."[1] This law reauthorized Section 702 of the Foreign Intelligence Surveillance Act for two years with various reforms. We write to request information regarding your implementation of certain reforms.

During consideration of H.R. 7888, the House of Representatives adopted an amendment offered by Representative Roy that, among other things, provided certain Members of Congress with access to the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISC-R) proceedings.[2] This provision provides Congress with vital and much-needed oversight of the FISA program. Indeed, during debate on the amendment, Representative Roy stated that the amendment's purpose was to give certain members and staff the ability "to observe the FISC, to be able to understand what is happening there, and be able to come back here so Congress can know what is happening to protect the American people."[3]

In order to further our oversight, we request that you arrange for the Justice Department to brief Committee staff about your progress on establishing procedures governing access to the FISC and FISC-R. We ask that you please direct your staff to work with Committee staff to schedule this briefing as soon as possible, but no later than 5:00 p.m. on June 11, 2024.

---

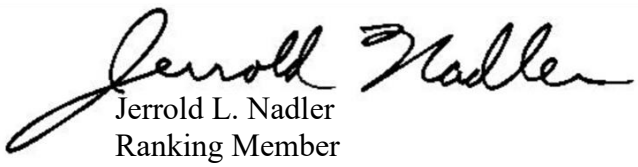
[1] PRESIDENTIAL ACTIONS, BILL SIGNED: H.R. 7888, THE WHITE HOUSE (Apr. 20, 2024).
[2] H.R. 7888, Roll no. 115, 118th CONG. (2024). Specifically, this provision allows the chair and ranking minority member of each of the congressional intelligence committees, the chairs and ranking members of the Committees on the Judiciary of the House of Representatives and of the Senate, the Majority and Minority Leaders of the Senate, the Speaker of the House of Representatives, and the Minority Leader of the House of Representatives to attend any proceeding of the FISC or FISC-R. The provision requires the Attorney General, in consultation with the Director of National Intelligence, to establish procedures for such attendance at these proceedings.
[3] 170 CONG. REC. H2348 (daily ed. Apr. 12, 2024) (statement of Rep. Roy).

Thank you for your prompt attention to this matter.

Sincerely,



Jim Jordan
Chairman



Jerrold L. Nadler
Ranking Member

JIM JORDAN, Ohio
CHAIRMAN

JERROLD NADLER, New York
RANKING MEMBER

ONE HUNDRED EIGHTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON THE JUDICIARY
2138 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6216
(202) 225–6906
judiciary.house.gov

May 28, 2024

The Honorable Avril Haines
Director of National Intelligence
Office of the Director of National Intelligence
1500 Tysons McLean Drive
McLean, VA 22102

Dear Director Haines:

On April 20, 2024, President Biden signed into law H.R. 7888, the "Reforming Intelligence and Securing America Act."[1] This law reauthorized Section 702 of the Foreign Intelligence Surveillance Act for two years with various reforms. We write to request information regarding your implementation of certain reforms.

During consideration of H.R. 7888, the House of Representatives adopted an amendment offered by Representative Roy that, among other things, provided certain Members of Congress with access to the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISC-R) proceedings.[2] This provision provides Congress with vital and much-needed oversight of the FISA program. Indeed, during debate on the amendment, Representative Roy stated that the amendment's purpose was to give certain members and staff the ability "to observe the FISC, to be able to understand what is happening there, and be able to come back here so Congress can know what is happening to protect the American people."[3]

In order to further our oversight, we request that you arrange for the Office of the Director of National Intelligence to brief Committee staff about your progress on establishing procedures governing access to the FISC and FISC-R. We ask that you please direct your staff to work with Committee staff to schedule this briefing as soon as possible, but no later than 5:00 p.m. on June 11, 2024.

---

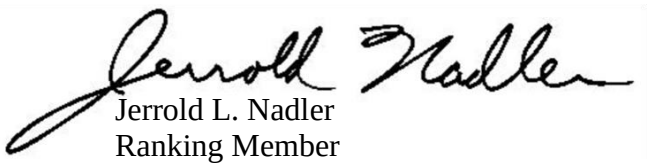
[1] PRESIDENTIAL ACTIONS, BILL SIGNED: H.R. 7888, THE WHITE HOUSE (Apr. 20, 2024).
[2] H.R. 7888, Roll no. 115, 118th CONG. (2024). Specifically, this provision allows the chair and ranking minority member of each of the congressional intelligence committees, the chairs and ranking members of the Committees on the Judiciary of the House of Representatives and of the Senate, the Majority and Minority Leaders of the Senate, the Speaker of the House of Representatives, and the Minority Leader of the House of Representatives to attend any proceeding of the FISC or FISC-R. The provision requires the Attorney General, in consultation with the Director of National Intelligence, to establish procedures for such attendance at these proceedings.
[3] 170 CONG. REC. H2348 (daily ed. Apr. 12, 2024) (statement of Rep. Roy).

Thank you for your prompt attention to this matter.

Sincerely,



Jim Jordan
Chairman



Jerrold L. Nadler
Ranking Member

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

The Honorable Zoe Lofgren
Co-Chair
Fourth Amendment Caucus
U.S. House of Representatives
Washington, DC 20515

Dear Representative Lofgren:

Thank you for your letter dated March 14, 2024, to the Department of Justice (Department) regarding Section 702 of the Foreign Intelligence Surveillance Act (FISA). We appreciate your interest in this issue. We are sending identical responses to the other Members who joined your letter.

Section 702 provides critical and unique foreign intelligence at a speed and reliability that the Intelligence Community cannot replicate with any other authority. The Department and the Office of the Director of National Intelligence transmitted a letter to Congress on April 5, 2024,[1] noting that the Foreign Intelligence Surveillance Court (FISC) had approved new certifications and legal procedures under the law that are valid until April 2025. In the letter the government committed to incorporating on an expedited timeline any additional reforms Congress enacted in connection with reauthorizing Section 702. That commitment included returning to the FISC as soon as practicable, but no later than 90 days after enactment of a reauthorization statute, to seek approval of new draft certifications and procedures that reflect any new statutory requirements.

On April 20, Congress passed the Reforming Intelligence and Securing America Act (RISAA), which extended Section 702 until April 2026 and included a number of significant reforms to the program.[2] Section 21 of RISAA requires the government to return to the FISC within 90 days for approval of new certifications and procedures that incorporate the reforms contained in the statute.[3] The Department intends to fully comply with this requirement.

[1] Letter from Dep't of Justice & Office of Director of Nat'l Intelligence (Apr. 5, 2024), https://www.justice.gov/nsd/media/1346981/dl?inline=.
[2] *See* Reforming Intelligence and Securing America Act (RISAA), Pub. L. 118-49 § 19.
[3] *See id.* § 21.

We appreciate your interest in protecting Americans' civil liberties and hope this information is helpful. We look forward to working with Congress to ensure the use of Section 702 reflects both a reverence for these cherished rights and due regard for our national security. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

CARLOS URIARTE

Digitally signed by CARLOS URIARTE
Date: 2024.05.10 16:02:58 -04'00'

Carlos Felipe Uriarte
Assistant Attorney General

cc:

The Honorable Mike Johnson
Speaker
U.S. House of Representatives
Washington, DC 20515

The Honorable Hakeem Jeffries
Minority Leader
U.S. House of Representatives
Washington, DC 20515

From: "Uriarte, Carlos F. (OLA)" (b) (6)
To: "Howard, Adam" (b) (6)
Subject: RE: Follow Up re Section 21
Date: Tue, 13 Feb 2024 09:33:42 -0500
Importance: Normal
Attachments: SEC._21._Information_Submission_2.13.24.pdf

Here you go.

From: Howard, Adam (b) (6)
Sent: Tuesday, February 13, 2024 9:27 AM
To: Uriarte, Carlos F. (OLA) (b) (6)
Subject: [EXTERNAL] RE: Follow Up re Section 21

Can you give me a call on my direct line (b) (6)

From: Uriarte, Carlos F. (OLA) (b) (6)
Sent: Monday, February 12, 2024 9:51 PM
To: Howard, Adam (b) (6)
Cc: Bond, Slade (OLA) (b) (6) ; (b) (6) (OLA) (b) (6)
Subject: Follow Up re Section 21

Adam,

Attached please find a one-pager from DOJ on Section 21, “Information Submission,” in the Reforming Intelligence and Securing America Act. Hopefully, this does the trick.

If you need a formal letter, just let me know and I will do my best to get you something tomorrow am.

Best,
Carlos

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

H.R. ___ - Reforming Intelligence and Securing America Act

SEC. 21. Information Submission

The Department of Justice objects to the inclusion of Section 21, titled "Information Submission," in the Reforming Intelligence and Securing America Act. This addition to the Reforming Intelligence and Securing America Act, a bill ostensibly intended to reauthorize Title VII of the Foreign Intelligence Surveillance Act (FISA), is unnecessary and undermines the primary purpose of the legislation. This provision is fundamentally unrelated to FISA Section 702, which authorizes foreign intelligence targeting of non-U.S. persons located overseas. Including this provision in a bill to reauthorize Section 702 creates the false and misleading perception that Section 702, or other provisions of Title VII, are focused on targeting U.S. persons or involve the purchase of commercially available data.

24cv3373_24-02439_000008

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

H.R. ___ - Reforming Intelligence and Securing America Act

SEC. 21. Information Submission

The Department of Justice objects to the inclusion of Section 21, titled "Information Submission," in the Reforming Intelligence and Securing America Act. This addition to the Reforming Intelligence and Securing America Act, a bill ostensibly intended to reauthorize Title VII of the Foreign Intelligence Surveillance Act (FISA), is unnecessary and undermines the primary purpose of the legislation. This provision is fundamentally unrelated to FISA Section 702, which authorizes foreign intelligence targeting of non-U.S. persons located overseas. Including this provision in a bill to reauthorize Section 702 creates the false and misleading perception that Section 702, or other provisions of Title VII, are focused on targeting U.S. persons or involve the purchase of commercially available data. Finally, this section unnecessarily clarifies that the Director of National Intelligence may submit information to Congress regarding the purchase of commercially available data about United States persons by law enforcement agencies and the intelligence community.

24cv3373_24-02439_000009

From: "Uriarte, Carlos F. (OLA)" <(b) (6) >
To: "Wu, William (Intelligence)" <(b) (6)
(b)(6) Eric Losick (Senate-SSCI)
Cc: "Bond, Slade (OLA)" (b) (6)
Subject: Letter
Date: Thu, 18 Apr 2024 11:57:10 -0400
Importance: Normal
Attachments: AG_Letter_4.18.2024_Schumer_and_McConnell.pdf

Office of the Attorney General
Washington, D. C. 20530

April 18, 2024

The Honorable Charles E. Schumer
Majority Leader
United States Senate
Washington, DC 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, DC 20510

Dear Leader Schumer and Leader McConnell:

As I testified yesterday, I urge the Senate to reauthorize Section 702 of the Foreign Intelligence Surveillance Act (FISA) before it expires on Friday. Section 702 is indispensable to our work to protect the American people from cyber, nation state, terrorist, and other threats.

Section 25 of H.R. 7888 includes language modifying the definition of "electronic communication service provider" (ECSP). As I testified yesterday, this is a technical amendment to address the changes in internet technology in the 15 years since Section 702 was passed. It is narrowly tailored and is in response to the Foreign Intelligence Surveillance Court's identification of a need for a legislative fix.

The attached April 17, 2024, letter from Assistant Attorney General Carlos Felipe Uriarte, including the Department of Justice's representations regarding the ECSP provision, reflects my views and my strong support for the passage of H.R. 7888.

Sincerely,

Merrick B. Garland
Attorney General

cc: The Honorable Mark Warner, Chairman, Select Committee on Intelligence, United States Senate

The Honorable Marco Rubio, Vice Chairman, Select Committee on Intelligence, United States Senate

The Honorable Richard J. Durbin, Chair, Committee on the Judiciary, United States Senate

The Honorable Lindsey O. Graham, Ranking Member, Committee on the Judiciary, United States Senate

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

The Honorable Mark Warner
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Warner:

We are grateful that the Senate is continuing to work on a bipartisan basis to extend Title VII of the Foreign Intelligence Surveillance Act (FISA), including Section 702, for an additional two years. Section 702 provides critical and unique foreign intelligence at a speed and reliability that the Intelligence Community cannot replicate with any other authority. The Intelligence Community relies on Section 702 in almost every aspect of its work, and the authority is essential to our national security.

We urge the Senate to pass H.R. 7888 by Friday, April 19. Doing so will prevent the lapse of this critical national security tool and will impose the most comprehensive set of reforms in the history of the Section 702 program.

As you are aware, Section 25 of H.R. 7888 includes technical language modifying the definition of "electronic communication service provider" (ECSP) to address unforeseen changes in electronic communications technology. As Attorney General Merrick Garland testified, this change "is a technical change. It's a consequence of internet technology changing in the 15 years since FISA 702 was passed. It's narrowly tailored. It is actually a response to a suggestion from the FISA court to make–to seek this kind of legislative fix. It does not in any way change who can be a target of Section 702."[1] This definition has not been updated since 2008 when Congress first enacted Section 702. The technical modification is intended to fill a critical intelligence gap—which was the subject of litigation before the Foreign Intelligence Surveillance Court (FISC)—regarding the types of communications services used by non-U.S. persons outside the United States.

[1] *A Review of the President's Fiscal Year 2025 Budget Request for the U.S. Department of Justice: Hearing Before the Commerce, Justice, Science, and Related Agencies Subcomm. to the S. Appropriations Comm.*, 118th Cong. (Apr. 17, 2024) (testimony of Attorney General Merrick Garland).

To address concerns some have raised about this amendment to the ECSP definition, the Department of Justice (Department) provides the following representations:

1. This technical change to the definition of ECSP does not affect the overall structure of Section 702 or the protections imposed on all aspects of the 702 program, including the court-imposed legal procedures. The targeting procedures under Section 702 strictly prohibit targeting persons or entities inside the United States or Americans anywhere in the world. The procedures further prohibit "reverse targeting," which is collecting on foreigners outside the United States for the purpose of obtaining the communications of a person inside the United States or of a U.S. person. **Accordingly, it would be unlawful under Section 702 to use the modified definition of ECSP to target any entity inside the United States including, for example, any business, home, or place of worship. It would also be unlawful to compel any service provider to target the communications of any person inside the United States, regardless of whether such a person is in contact with a non-U.S. person outside the United States.** Some critics have falsely suggested that the amended definition of ECSP could be used to conduct surveillance at churches or media companies in the United States—this activity would be legally barred under the rules governing targeting under Section 702 and the prohibition against targeting anyone inside the United States.

2. **Further, the Department commits to applying this definition of ECSP exclusively to cover the type of service provider at issue in the litigation before the FISC—that is, technology companies that provide the service the FISC concluded fell outside the current definition.** The number of technology companies providing this service is extremely small, and we will identify these technology companies to Congress in a classified appendix. To protect sensitive sources and methods, the ECSP provision in H.R. 7888 was drafted to avoid unnecessarily alerting foreign adversaries to sensitive collection techniques.

3. As you are aware, the government provides Congress with a copy of all Section 702 directives issued to U.S. electronic communication service providers. **To facilitate appropriate oversight and transparency of the government's commitment to apply any updated definition of ECSP only for the limited purposes described above, the Department will also report to Congress every six months regarding any applications of the updated definition.** This additional reporting will allow Congress to ensure the government adheres to our commitment regarding the narrow application of this definition.

Congress plays a critical role in the ongoing oversight of the government's use of Section 702. We look forward to continuing to work with Congress to reauthorize this critical national security tool to protect our national security while safeguarding privacy and civil liberties.

Sincerely,

CARLOS URIARTE

Digitally signed by CARLOS URIARTE
Date: 2024.04.17 22:40:35 -04'00'

Carlos Felipe Uriarte
Assistant Attorney General

cc:

The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

From: "Uriarte, Carlos F. (OLA)" (b) (6)
To: "Wu, William (Intelligence)" (b) (6)
Subject: Letter
Date: Wed, 17 Apr 2024 22:42:02 -0400
Importance: Normal
Attachments: 2024.04.17-OUT-Warner-ECSP_Commitment.pdf

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, DC 20530*

The Honorable Mark Warner
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Chairman Warner:

We are grateful that the Senate is continuing to work on a bipartisan basis to extend Title VII of the Foreign Intelligence Surveillance Act (FISA), including Section 702, for an additional two years. Section 702 provides critical and unique foreign intelligence at a speed and reliability that the Intelligence Community cannot replicate with any other authority. The Intelligence Community relies on Section 702 in almost every aspect of its work, and the authority is essential to our national security.

We urge the Senate to pass H.R. 7888 by Friday, April 19. Doing so will prevent the lapse of this critical national security tool and will impose the most comprehensive set of reforms in the history of the Section 702 program.

As you are aware, Section 25 of H.R. 7888 includes technical language modifying the definition of "electronic communication service provider" (ECSP) to address unforeseen changes in electronic communications technology. As Attorney General Merrick Garland testified, this change "is a technical change. It's a consequence of internet technology changing in the 15 years since FISA 702 was passed. It's narrowly tailored. It is actually a response to a suggestion from the FISA court to make–to seek this kind of legislative fix. It does not in any way change who can be a target of Section 702."[1] This definition has not been updated since 2008 when Congress first enacted Section 702. The technical modification is intended to fill a critical intelligence gap—which was the subject of litigation before the Foreign Intelligence Surveillance Court (FISC)—regarding the types of communications services used by non-U.S. persons outside the United States.

[1] *A Review of the President's Fiscal Year 2025 Budget Request for the U.S. Department of Justice: Hearing Before the Commerce, Justice, Science, and Related Agencies Subcomm. to the S. Appropriations Comm.*, 118th Cong. (Apr. 17, 2024) (testimony of Attorney General Merrick Garland).

To address concerns some have raised about this amendment to the ECSP definition, the Department of Justice (Department) provides the following representations:

1. This technical change to the definition of ECSP does not affect the overall structure of Section 702 or the protections imposed on all aspects of the 702 program, including the court-imposed legal procedures. The targeting procedures under Section 702 strictly prohibit targeting persons or entities inside the United States or Americans anywhere in the world. The procedures further prohibit "reverse targeting," which is collecting on foreigners outside the United States for the purpose of obtaining the communications of a person inside the United States or of a U.S. person. **Accordingly, it would be unlawful under Section 702 to use the modified definition of ECSP to target any entity inside the United States including, for example, any business, home, or place of worship. It would also be unlawful to compel any service provider to target the communications of any person inside the United States, regardless of whether such a person is in contact with a non-U.S. person outside the United States.** Some critics have falsely suggested that the amended definition of ECSP could be used to conduct surveillance at churches or media companies in the United States—this activity would be legally barred under the rules governing targeting under Section 702 and the prohibition against targeting anyone inside the United States.

2. **Further, the Department commits to applying this definition of ECSP exclusively to cover the type of service provider at issue in the litigation before the FISC—that is, technology companies that provide the service the FISC concluded fell outside the current definition.** The number of technology companies providing this service is extremely small, and we will identify these technology companies to Congress in a classified appendix. To protect sensitive sources and methods, the ECSP provision in H.R. 7888 was drafted to avoid unnecessarily alerting foreign adversaries to sensitive collection techniques.

3. As you are aware, the government provides Congress with a copy of all Section 702 directives issued to U.S. electronic communication service providers. **To facilitate appropriate oversight and transparency of the government's commitment to apply any updated definition of ECSP only for the limited purposes described above, the Department will also report to Congress every six months regarding any applications of the updated definition.** This additional reporting will allow Congress to ensure the government adheres to our commitment regarding the narrow application of this definition.

Congress plays a critical role in the ongoing oversight of the government's use of Section 702. We look forward to continuing to work with Congress to reauthorize this critical national security tool to protect our national security while safeguarding privacy and civil liberties.

Sincerely,

CARLOS URIARTE

Digitally signed by CARLOS URIARTE
Date: 2024.04.17 22:40:35 -04'00'

Carlos Felipe Uriarte
Assistant Attorney General

cc:

The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

From: "Losick, Eric (Intelligence)" <(b) (6)
To: "Uriarte, Carlos F. (OLA)" <(b) (6) "Bond, Slade (OLA)" <(b) (6)
Cc: "Fisher, Janet (Intelligence)" <(b) (6)
Subject: [EXTERNAL] Text of FY25 IAA as filed
Date: Mon, 03 Jun 2024 17:36:29 -0400
Importance: Normal
Attachments: BAG24915.pdf; BAG24915.docx

Please find attached the text of the Intelligence Authorization Act for Fiscal Year 2025, as filed earlier today. This text will likely take a day or two to appear on congress.gov. Happy to discuss as may be helpful.

Eric Losick
General Counsel
Senate Select Committee on Intelligence
(b) (6)

Calendar No. _____

118TH CONGRESS
2D SESSION

S. _____

[Report No. 118–_____]

To authorize appropriations for fiscal year 2025 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

---

A BILL

To authorize appropriations for fiscal year 2025 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Intelligence Authorization Act for Fiscal Year 2025''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—INTELLIGENCE ACTIVITIES

Sec. 101. Authorization of appropriations.
Sec. 102. Classified Schedule of Authorizations.
Sec. 103. Intelligence Community Management Account.
Sec. 104. Increase in employee compensation and benefits authorized by law.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Sec. 201. Authorization of appropriations.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

Sec. 301. Improvements relating to conflicts of interest in the Intelligence Innovation Board.
Sec. 302. National Threat Identification and Prioritization Assessment and National Counterintelligence Strategy.
Sec. 303. Open Source Intelligence Division of Office of Intelligence and Analysis personnel.
Sec. 304. Appointment of Director of the Office of Intelligence and Counterintelligence.
Sec. 305. Improvements to advisory board of National Reconnaissance Office.
Sec. 306. National Intelligence University acceptance of grants.
Sec. 307. Protection of Central Intelligence Agency facilities and assets from unmanned aircraft.
Sec. 308. Limitation on availability of funds for new controlled access programs.
Sec. 309. Limitation on transfers from controlled access programs.
Sec. 310. Expenditure of funds for certain intelligence and counterintelligence activities of the Coast Guard.
Sec. 311. Unauthorized access to intelligence community property.
Sec. 312. Strengthening of Office of Intelligence and Analysis.
Sec. 313. Report on sensitive commercially available information.
Sec. 314. Policy on collection of United States location information.
Sec. 315. Display of flags, seals, and emblems other than the United States flag.

TITLE IV—COUNTERING FOREIGN THREATS

Subtitle A—People's Republic of China

Sec. 401. Strategy and outreach on risks posed by People's Republic of China smartport technology.
Sec. 402. Assessment of current status of biotechnology of People's Republic of China.
Sec. 403. Intelligence sharing with law enforcement agencies on synthetic opioid precursor chemicals originating in People's Republic of China.
Sec. 404. Report on efforts of the People's Republic of China to evade United States transparency and national security regulations.

Sec. 405. Plan for recruitment of Mandarin speakers.

Subtitle B—The Russian Federation

Sec. 411. Assessment of Russian Federation sponsorship of acts of international terrorism.
Sec. 412. Assessment of likely course of war in Ukraine.

Subtitle C—International Terrorism

Sec. 421. Inclusion of Hamas, Hezbollah, Al-Qaeda, and ISIS officials and members among aliens engaged in terrorist activity.
Sec. 422. Assessment and report on the threat of ISIS-Khorasan to the United States.
Sec. 423. Terrorist financing prevention.

Subtitle D—Other Foreign Threats

Sec. 431. Assessment of visa-free travel to and within Western Hemisphere by nationals of countries of concern.
Sec. 432. Study on threat posed by foreign investment in United States agricultural land.
Sec. 433. Assessment of threat posed by citizenship-by-investment programs.
Sec. 434. Mitigating the use of United States components and technology in hostile activities by foreign adversaries.
Sec. 435. Office of Intelligence and Counterintelligence review of visitors and assignees.
Sec. 436. Prohibition on National Laboratories admitting certain foreign nationals.
Sec. 437. Quarterly report on certain foreign nationals encountered at the United States border.
Sec. 438. Assessment of the lessons learned by the intelligence community with respect to the Israel-Hamas war.
Sec. 439. Central Intelligence Agency intelligence assessment on Tren de Aragua.
Sec. 440. Assessment of Maduro regime's economic and security relationships with state sponsors of terrorism and foreign terrorist organizations.
Sec. 441. Continued congressional oversight of Iranian expenditures supporting foreign military and terrorist activities.

TITLE V—EMERGING TECHNOLOGIES

Sec. 501. Strategy to counter foreign adversary efforts to utilize biotechnologies in ways that threaten United States national security.
Sec. 502. Improvements to the roles, missions, and objectives of the National Counterproliferation and Biosecurity Center.
Sec. 503. Enhancing capabilities to detect foreign adversary threats relating to biological data.
Sec. 504. National security procedures to address certain risks and threats relating to artificial intelligence.
Sec. 505. Establishment of Artificial Intelligence Security Center.
Sec. 506. Sense of Congress encouraging intelligence community to increase private sector capital partnerships and partnership with Office of Strategic Capital of Department of Defense to secure enduring technological advantages.
Sec. 507. Intelligence Community Technology Bridge Fund.

Sec. 508. Enhancement of authority for intelligence community public-private talent exchanges.
Sec. 509. Enhancing intelligence community ability to acquire emerging technology that fulfills intelligence community needs.
Sec. 510. Management of artificial intelligence security risks.
Sec. 511. Protection of technological measures designed to verify authenticity or provenance of machine-manipulated media.
Sec. 512. Sense of Congress on hostile foreign cyber actors.
Sec. 513. Designation of state sponsors of ransomware and reporting requirements.
Sec. 514. Deeming ransomware threats to critical infrastructure a national intelligence priority.

TITLE VI—CLASSIFICATION REFORM

Sec. 601. Governance of classification and declassification system.
Sec. 602. Classification and declassification of information.
Sec. 603. Minimum standards for Executive agency insider threat programs.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

Sec. 701. Security clearances held by certain former employees of intelligence community.
Sec. 702. Policy for authorizing intelligence community program of contractor-owned and contractor-operated sensitive compartmented information facilities.
Sec. 703. Enabling intelligence community integration.
Sec. 704. Appointment of spouses of certain Federal employees.
Sec. 705. Plan for staffing the intelligence collection positions of the Central Intelligence Agency.
Sec. 706. Intelligence community workplace protections.
Sec. 707. Sense of Congress on Government personnel support for foreign terrorist organizations.

TITLE VIII—WHISTLEBLOWERS

Sec. 801. Improvements regarding urgent concerns submitted to Inspectors General of the intelligence community.
Sec. 802. Prohibition against disclosure of whistleblower identity as act of reprisal.
Sec. 803. Protection for individuals making authorized disclosures to Inspectors General of elements of the intelligence community.
Sec. 804. Clarification of authority of certain Inspectors General to receive protected disclosures.
Sec. 805. Whistleblower protections relating to psychiatric testing or examination.
Sec. 806. Establishing process parity for adverse security clearance and access determinations.
Sec. 807. Elimination of cap on compensatory damages for retaliatory revocation of security clearances and access determinations.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

Sec. 901. Additional discretion for Director of Central Intelligence Agency in paying costs of treating qualifying injuries and making payments for qualifying injuries to the brain.

Sec. 902. Additional discretion for Secretary of State and heads of other Federal agencies in paying costs of treating qualifying injuries and making payments for qualifying injuries to the brain.
Sec. 903. Improved funding flexibility for payments made by Department of State for qualifying injuries to the brain.

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

Sec. 1001. Comptroller General of the United States review of All-domain Anomaly Resolution Office.
Sec. 1002. Sunset of requirements relating to audits of unidentified anomalous phenomena historical record report.
Sec. 1003. Funding limitations relating to unidentified anomalous phenomena.

TITLE XI—AIR AMERICA

Sec. 1101. Short title.
Sec. 1102. Findings.
Sec. 1103. Definitions.
Sec. 1104. Award authorized to eligible persons.
Sec. 1105. Funding limitation.
Sec. 1106. Time limitation.
Sec. 1107. Application procedures.
Sec. 1108. Rule of construction.
Sec. 1109. Attorneys' and agents' fees.
Sec. 1110. No judicial review.
Sec. 1111. Reports to Congress.

TITLE XII—OTHER MATTERS

Sec. 1201. Enhanced authorities for amicus curiae under the Foreign Intelligence Surveillance Act of 1978.
Sec. 1202. Limitation on directives under Foreign Intelligence Surveillance Act of 1978 relating to certain electronic communication service providers.
Sec. 1203. Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024.
Sec. 1204. Privacy and Civil Liberties Oversight Board qualifications.
Sec. 1205. Parity in pay for staff of the Privacy and Civil Liberties Oversight Board and the intelligence community.
Sec. 1206. Modification and repeal of reporting requirements.
Sec. 1207. Technical amendments.

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term ''congressional intelligence committees'' has the meaning given such term in section

3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in such section.

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2025 for the conduct of the intelligence and intelligence-related activities of the Federal Government.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) SPECIFICATIONS OF AMOUNTS.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the Federal Government are those specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) AVAILABILITY OF CLASSIFIED SCHEDULE OF AUTHORIZATIONS.—

(1) AVAILABILITY.—The classified Schedule of Authorizations referred to in subsection (a) shall be made available to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and to the President.

(2) DISTRIBUTION BY THE PRESIDENT.—Subject to paragraph (3), the President shall provide for suitable distribution of the classified Schedule of Authorizations referred to in subsection (a), or of appropriate portions of such Schedule, within the executive branch of the Federal Government.

(3) LIMITS ON DISCLOSURE.—The President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule except—

(A) as provided in section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a));

(B) to the extent necessary to implement the budget; or

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2025 the sum of $656,573,000.

(b) CLASSIFIED AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Ac-

count by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2025 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

SEC. 104. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

Appropriations authorized by this Act for salary, pay, retirement, and other benefits for Federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in such compensation or benefits authorized by law.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2025.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

SEC. 301. IMPROVEMENTS RELATING TO CONFLICTS OF INTEREST IN THE INTELLIGENCE INNOVATION BOARD.

Section 7506(g) of the Intelligence Authorization Act for Fiscal Year 2024 (Public Law 118–31) is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by inserting ''active and'' before ''potential'';

(B) in subparagraph (B), by striking ''the Inspector General of the Intelligence Community'' and inserting ''the designated agency ethics official'';

(C) by redesignating subparagraph (C) as subparagraph (D); and

(D) by inserting after subparagraph (B) the following:

''(C) Authority for the designated agency ethics official to grant a waiver for a conflict of interest, except that—

''(i) no waiver may be granted for an active conflict of interest identified with respect to the Chair of the Board;

"(ii) every waiver for a potential conflict of interest requires review and approval by the Director of National Intelligence; and

"(iii) for every waiver granted, the designated agency ethics official shall submit to the congressional intelligence committees notice of the waiver."; and

(2) by adding at the end the following:

"(3) DEFINITION OF DESIGNATED AGENCY ETHICS OFFICIAL.—In this subsection, the term 'designated agency ethics official' means the designated agency ethics official (as defined in section 13101 of title 5, United States Code) in the Office of the Director of National Intelligence.".

SEC. 302. NATIONAL THREAT IDENTIFICATION AND PRIORITIZATION ASSESSMENT AND NATIONAL COUNTERINTELLIGENCE STRATEGY.

Section 904(f)(3) of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3383(f)(3)) is amended by striking "National Counterintelligence Executive" and inserting "Director of the National Counterintelligence and Security Center".

SEC. 303. OPEN SOURCE INTELLIGENCE DIVISION OF OFFICE OF INTELLIGENCE AND ANALYSIS PERSONNEL.

None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2025 for the Office of Intelligence and Analysis of the Department of Homeland Security may be obligated or expended by the Office to increase, above the staffing level in effect on the day before the date of the enactment of this Act, the number of personnel assigned to the Open Source Intelligence Division who work exclusively or predominantly on domestic terrorism issues.

SEC. 304. APPOINTMENT OF DIRECTOR OF THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE.

(a) IN GENERAL.—Section 215(c) of the Department of Energy Organization Act (42 U.S.C. 7144b(c)) is amended to read as follows:

''(c) DIRECTOR.—

''(1) APPOINTMENT.—The head of the Office shall be the Director of the Office of Intelligence and Counterintelligence, who shall be appointed by the President, by and with the advice and consent of the Senate. The Director of the Office shall report directly to the Secretary.

''(2) TERM.—

"(A) IN GENERAL.—The Director shall serve for a term of 6 years.

"(B) REAPPOINTMENT.—The Director shall be eligible for reappointment for 1 or more terms.

"(3) QUALIFICATIONS.—The Director shall—

"(A) be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate; and

"(B) have substantial expertise in matters relating to the intelligence community, including foreign intelligence and counterintelligence.".

(b) EFFECTIVE DATE.—The amendment made by this section shall take effect on January 21, 2025.

SEC. 305. IMPROVEMENTS TO ADVISORY BOARD OF NATIONAL RECONNAISSANCE OFFICE.

Section 106A(d) of the National Security Act of 1947 (50 U.S.C. 3041a(d)) is amended—

(1) in paragraph (3)(A)—

(A) in clause (i)—

(i) by striking ''five members appointed by the Director, in consultation with the Director of National Intelligence and the Secretary of Defense,'' and inserting ''up to 8 members appointed by the Director''; and

(ii) by inserting '', and who do not present any actual or potential conflict of interest'' before the period at the end;

(B) by redesignating clause (ii) as clause (iii); and

(C) by inserting after clause (i) the following:

''(ii) MEMBERSHIP STRUCTURE.—The Director shall ensure that no more than 2 concurrently serving members of the Board qualify for membership on the Board based predominantly on a single qualification set forth under clause (i).'';

(2) by redesignating paragraphs (5) through (7) as paragraphs (6) through (8), respectively;

(3) by inserting after paragraph (4) the following:

''(5) CHARTER.—The Director shall establish a charter for the Board that includes the following:

"(A) Mandatory processes for identifying potential conflicts of interest, including the submission of initial and periodic financial disclosures by Board members.

"(B) The vetting of potential conflicts of interest by the designated agency ethics official, except that no individual waiver may be granted for a conflict of interest identified with respect to the Chair of the Board.

"(C) The establishment of a process and associated protections for any whistleblower alleging a violation of applicable conflict of interest law, Federal contracting law, or other provision of law."; and

(4) in paragraph (8), as redesignated by paragraph (2), by striking "September 30, 2024" and inserting "August 31, 2027".

SEC. 306. NATIONAL INTELLIGENCE UNIVERSITY ACCEPTANCE OF GRANTS.

(a) IN GENERAL.—Subtitle D of title X of the National Security Act of 1947 (50 U.S.C. 3227 et seq.) is amended by adding at the end the following:

"§ 1035. National Intelligence University acceptance of grants

''(a) AUTHORITY.—The Director of National Intelligence may authorize the President of the National Intelligence University to accept qualifying research grants.

''(b) QUALIFYING GRANTS.—A qualifying research grant under this section is a grant that is awarded on a competitive basis by an entity referred to in subsection (c) for a research project with a scientific, literary, or educational purpose.

''(c) ENTITIES FROM WHICH GRANTS MAY BE ACCEPTED.—A qualifying research grant may be accepted under this section only from a Federal agency or from a corporation, fund, foundation, educational institution, or similar entity that is organized and operated primarily for scientific, literary, or educational purposes.

''(d) ADMINISTRATION OF GRANT FUNDS.—

''(1) ESTABLISHMENT OF ACCOUNT.—The Director shall establish an account for administering funds received as qualifying research grants under this section.

''(2) USE OF FUNDS.—The President of the University shall use the funds in the account established pursuant to paragraph (1) in accordance with applicable provisions of the regulations and the terms and conditions of the grants received.

''(e) RELATED EXPENSES.—Subject to such limitations as may be provided in appropriations Acts, appropriations available for the National Intelligence University may be used to pay expenses incurred by the University in applying for, and otherwise pursuing, the award of qualifying research grants.

''(f) REGULATIONS.—The Director of National Intelligence shall prescribe regulations for the administration of this section.''.

(b) CLERICAL AMENDMENT.—The table of contents preceding section 2 of such Act is amended by inserting after the item relating to section 1034 the following new item:

''Sec. 1035. National Intelligence University acceptance of grants.''.

SEC. 307. PROTECTION OF CENTRAL INTELLIGENCE AGENCY FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by inserting after section 15 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

''SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

''(a) DEFINITIONS.—In this section:

''(1) BUDGET.—The term 'budget', with respect to a fiscal year, means the budget for that fiscal

year that is submitted to Congress by the President under section 1105(a) of title 31, United States Code.

''(2) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

''(A) the Select Committee on Intelligence of the Senate;

''(B) the Permanent Select Committee on Intelligence of the House of Representatives;

''(C) the Subcommittee on Defense of the Committee on Appropriations of the Senate; and

''(D) the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

''(3) CONGRESSIONAL JUDICIARY COMMITTEES.—The term 'congressional judiciary committees' means—

''(A) the Committee on the Judiciary of the Senate; and

''(B) the Committee on the Judiciary of the House of Representatives.

''(4) CONGRESSIONAL TRANSPORTATION AND INFRASTRUCTURE COMMITTEES.—The term 'con-

gressional transportation and infrastructure committees' means—

"(A) the Committee on Commerce, Science, and Transportation of the Senate; and

"(B) the Committee on Transportation and Infrastructure of the House of Representatives.

"(5) COVERED FACILITY OR ASSET.—The term 'covered facility or asset' means property owned, leased, or controlled by the Agency, property controlled and occupied by the Federal Highway Administration, located immediately adjacent to the headquarters compound of the Agency, and property owned, leased, or controlled by the Office of the Director of National Intelligence where the property—

"(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Director, in coordination with the Secretary of Transportation, with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

"(B) is located in the United States and beneath airspace that is prohibited or restricted by the Federal Aviation Administration;

''(C) is a property of which Congress has been notified is covered under this paragraph; and

''(D) directly relates to one or more functions authorized to be performed by the Agency, pursuant to the National Security Act of 1947 (50 U.S.C. 3001) or this Act.

''(6) ELECTRONIC COMMUNICATION.—The term 'electronic communication' has the meaning given such term in section 2510 of title 18, United States Code.

''(7) INTERCEPT.—The term 'intercept' has the meaning given such term in section 2510 of title 18, United States Code.

''(8) ORAL COMMUNICATION.—The term 'oral communication' has the meaning given such term in section 2510 of title 18, United States Code.

''(9) RADIO COMMUNICATION.—The term 'radio communication' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

''(10) RISK-BASED ASSESSMENT.—The term 'risk-based assessment' includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the

safety and efficiency of the National Airspace System and the needs of national security at each covered facility or asset identified by the Director, an evaluation of each of the following factors:

"(A) Potential impacts to safety, efficiency, and use of the National Airspace System, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services relating to the use of any system or technology for carrying out the actions described in subsection (c)(1).

"(B) Options for mitigating any identified impacts to the National Airspace System relating to the use of any system or technology, including minimizing when possible the use of any system or technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

"(C) Potential consequences of the effects of any actions taken under subsection (c)(1) to the National Airspace System and infrastructure if not mitigated.

"(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the National Airspace System and the needs of national security.

"(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, and any potential for interference with wireless communications or for injury or damage to persons or property.

"(F) Potential consequences to national security if threats posed by unmanned aircraft systems or unmanned aircraft are not mitigated or defeated.

"(11) UNITED STATES.—The term 'United States' has the meaning given that term in section 5 of title 18, United States Code.

"(12) UNMANNED AIRCRAFT; UNMANNED AIRCRAFT SYSTEM.—The terms 'unmanned aircraft' and 'unmanned aircraft system' have the meanings given those terms in section 44801 of title 49, United States Code.

"(13) WIRE COMMUNICATION.—The term 'wire communication' has the meaning given such term in section 2510 of title 18, United States Code.

''(b) AUTHORITY.—Notwithstanding section 46502 of title 49, United States Code, or sections 32, 1030, and 1367 and chapters 119 and 206 of title 18, United States Code, or section 705 of the Communications Act of 1934 (47 U.S.C. 605), the Director may take, and may authorize Agency personnel with assigned duties that include the security or protection of people, facilities, or assets within the United States to take—

''(1) such actions described in subsection (c)(1) that are necessary to mitigate a credible threat (as defined by the Director, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset; and

''(2) such actions described in subsection (c)(3).

''(c) ACTIONS.—

''(1) ACTIONS DESCRIBED.—The actions described in this paragraph are the following:

''(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control

the unmanned aircraft system or unmanned aircraft.

"(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active and by direct or indirect physical, electronic, radio, or electromagnetic means.

"(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

"(D) Seize or exercise control over the unmanned aircraft system or unmanned aircraft.

"(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

"(F) Use reasonable force, if necessary, to seize or otherwise disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

"(2) COORDINATION.—The Director shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

"(3) RESEARCH, TESTING, TRAINING, AND EVALUATION.—

"(A) IN GENERAL.—The Director shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine the capability and utility of the equipment prior to the use of the equipment for any action described in paragraph (1).

"(B) PERSONNEL.—Personnel and contractors who do not have assigned duties that include the security or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to subparagraph (A).

"(4) FAA COORDINATION.—The Director shall coordinate with the Administrator of the Federal Aviation Administration on any action described in paragraph (1) or (3) so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely affect or interfere with safe airport operations, navigation, air

traffic services, or the safe and efficient operation of the National Airspace System.

''(d) FORFEITURE.—Any unmanned aircraft system or unmanned aircraft that is seized pursuant to subsection (b) as described in subsection (c)(1) is subject to forfeiture to the United States.

''(e) REGULATIONS AND GUIDANCE.—

''(1) ISSUANCE.—The Director and the Secretary of Transportation may each prescribe regulations, and shall each issue guidance, to carry out this section.

''(2) COORDINATION.—

''(A) REQUIREMENT.—The Director shall coordinate the development of guidance under paragraph (1) with the Secretary of Transportation.

''(B) AVIATION SAFETY.—The Director shall coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely affect or interfere with safe airport operations, navigation, air

traffic services, or the safe and efficient operation of the National Airspace System.

''(f) PRIVACY PROTECTION.—The regulations prescribed or guidance issued under subsection (e) shall ensure that—

''(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system or unmanned aircraft under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

''(2) communications to or from an unmanned aircraft system or unmanned aircraft are intercepted or acquired only to the extent necessary to support an action described in subsection (c);

''(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Director determines that maintenance of such records for a longer period is necessary for the investigation or prosecution of a violation of law, to fulfill a duty, responsibility, or function of the Agency, is required under Federal law, or for the purpose of any litigation; and

"(4) such communications are not disclosed outside the Agency unless the disclosure—

"(A) is necessary to investigate or prosecute a violation of law;

"(B) would support the Agency, the Department of Defense, a Federal law enforcement, intelligence, or security agency, a State, local, Tribal, or territorial law enforcement agency, or other relevant person or entity if such entity or person is engaged in a security or protection operation;

"(C) is necessary to support a department or agency listed in subparagraph (B) in investigating or prosecuting a violation of law;

"(D) would support the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory, statutory, or other enforcement action relating to, an action described in subsection (b);

"(E) is necessary to protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft;

"(F) is necessary to fulfill a duty, responsibility, or function of the Agency; or

"(G) is otherwise required by law.

"(g) BUDGET.—

"(1) IN GENERAL.—The Director shall submit to the congressional intelligence committees, as a part of the budget request of the Agency for each fiscal year after fiscal year 2025, a consolidated funding display that identifies the funding source for the actions described in subsection (c)(1) within the Agency.

"(2) FORM.—Each funding display submitted pursuant to paragraph (1) shall be in unclassified form, but may contain a classified annex.

"(h) SEMIANNUAL BRIEFINGS AND NOTIFICATIONS.—

"(1) BRIEFINGS.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 and semiannually thereafter, the Director shall provide the congressional intelligence committees, the congressional judiciary committees, and the congressional transportation and infrastructure committees a briefing on the activities carried out pursuant to this section during the period covered by the briefing.

''(2) REQUIREMENT.—Each briefing under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

''(3) CONTENTS.—Each briefing under paragraph (1) shall include, for the period covered by the briefing, the following:

''(A) Policies, programs, and procedures to mitigate or eliminate the effects of the activities described in paragraph (1) to the National Airspace System and other critical national transportation infrastructure.

''(B) A description of instances in which actions described in subsection (c)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property.

''(C) A description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues affected by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights, or civil liberties.

''(D) A description of options considered and steps taken to mitigate any identified ef-

fects on the National Airspace System relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

''(E) A description of instances in which communications intercepted or acquired during the course of operations of an unmanned aircraft system or unmanned aircraft were maintained for more than 180 days or disclosed outside the Agency.

''(F) How the Director and the Secretary of Transportation have informed the public as to the possible use of authorities under this section.

''(G) How the Director and the Secretary of Transportation have engaged with Federal, State, local, territorial, or Tribal law enforcement agencies to implement and use such authorities.

''(H) An assessment of whether any gaps or insufficiencies remain in statutes, regulations, and policies that impede the ability of the Agency to counter the threat posed by the mali-

cious use of unmanned aircraft systems and unmanned aircraft and any recommendations to remedy such gaps or insufficiencies.

''(4) FORM.—Each briefing under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified report.

''(5) NOTIFICATION.—

''(A) IN GENERAL.—Within 30 days of deploying any new technology to carry out the actions described in subsection (c)(1), the Director shall submit to the congressional intelligence committees a notification of the deployment of such technology.

''(B) CONTENTS.—Each notification submitted pursuant to subparagraph (A) shall include a description of options considered to mitigate any identified effects on the National Airspace System relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

''(i) RULE OF CONSTRUCTION.—Nothing in this section may be construed—

''(1) to vest in the Director any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration; or

''(2) to vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Director.

''(j) TERMINATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the authority to carry out this section with respect to the actions specified in subparagraphs (B) through (F) of subsection (c)(1), shall terminate on the date that is 4 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025.

''(2) EXTENSION.—The President may extend by 1 year the termination date specified in paragraph (1) if, before termination, the President certifies to Congress that such extension is in the national security interests of the United States.

''(k) SCOPE OF AUTHORITY.—Nothing in this section shall be construed to provide the Director or the Secretary of Transportation with additional authorities beyond those described in subsections (b) and (d).''.

SEC. 308. LIMITATION ON AVAILABILITY OF FUNDS FOR NEW CONTROLLED ACCESS PROGRAMS.

None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2025 for the National Intelligence Program may be obligated or expended for any controlled access program (as defined in section 501A(d) of the National Security Act of 1947 (50 U.S.C. 3091a(d))), or a compartment or subcompartment therein, that is established on or after the date of the enactment of this Act, until the head of the element of the intelligence community responsible for the establishment of such program, compartment, or subcompartment, submits the notification required by section 501A(b) of the National Security Act of 1947 (50 U.S.C. 3091a(b)).

SEC. 309. LIMITATION ON TRANSFERS FROM CONTROLLED ACCESS PROGRAMS.

Section 501A(b) of the National Security Act of 1947 (50 U.S.C. 3091a(b)) is amended—

(1) in the subsection heading, by striking ''LIMITATION ON ESTABLISHMENT'' and inserting ''LIMITATIONS'';

(2) by striking ''A head'' and inserting the following:

''(1) ESTABLISHMENT.—A head''; and

(3) by adding at the end the following:

''(2) TRANSFERS.—A head of an element of the intelligence community may not transfer a capability from a controlled access program, including from a compartment or subcompartment therein to a compartment or subcompartment of another controlled access program, to a special access program (as defined in section 1152(g) of the National Defense Authorization Act for Fiscal Year 1994 (50 U.S.C. 3348(g))), or to anything else outside the controlled access program, until the head submits to the appropriate congressional committees and congressional leadership notice of the intent of the head to make such transfer.''.

SEC. 310. EXPENDITURE OF FUNDS FOR CERTAIN INTELLIGENCE AND COUNTERINTELLIGENCE ACTIVITIES OF THE COAST GUARD.

The Commandant of the Coast Guard may use up to 1 percent of the amounts made available for the National Intelligence Program (as such term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) for each fiscal year for intelligence and counterintelligence activities of the Coast Guard relating to objects of a confidential, extraordinary, or emergency nature, which amounts may be accounted for solely on the certification of the Commandant and each such certification

shall be considered to be a sufficient voucher for the amount contained in the certification.

SEC. 311. UNAUTHORIZED ACCESS TO INTELLIGENCE COMMUNITY PROPERTY.

(a) IN GENERAL.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended by adding at the end the following:

"SEC. 1115. UNAUTHORIZED ACCESS TO INTELLIGENCE COMMUNITY PROPERTY.

''(a) IN GENERAL.—It shall be unlawful, within the jurisdiction of the United States, without authorization to access any property that—

''(1) is under the jurisdiction of an element of the intelligence community; and

''(2) has been clearly marked as closed or restricted.

''(b) PENALTIES.—Any person who violates subsection (a) shall—

''(1) in the case of the first offense, be fined under title 18, United States Code, imprisoned for not more than 180 days, or both;

''(2) in the case of the second offense, be fined under such title, imprisoned for not more than 3 years, or both; and

''(3) in the case of the third or subsequent offense, be fined under such title, imprisoned for not more than 10 years, or both.''.

(b) CLERICAL AMENDMENT.—The table of contents preceding section 2 of such Act is amended by adding at the end the following:

''Sec. 1115. Unauthorized access to intelligence community property.''.

SEC. 312. STRENGTHENING OF OFFICE OF INTELLIGENCE AND ANALYSIS.

(a) IN GENERAL.—Section 311 of title 31, United States Code, is amended to read as follows:

''§ 311. Office of Economic Intelligence and Security

''(a) DEFINITIONS.—In this section, the terms 'counterintelligence', 'foreign intelligence', and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(b) ESTABLISHMENT.—There is established within the Office of Terrorism and Financial Intelligence of the Department of the Treasury, the Office of Economic Intelligence and Security (in this section referred to as the 'Office'), which shall—

''(1) be responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information relating to the operation and responsibilities of the Department of the Treasury and other Federal agencies exe-

cuting economic statecraft tools that do not include any elements that are elements of the intelligence community;

''(2) provide intelligence support and economic analysis to Federal agencies implementing United States economic policy, including for purposes of global strategic competition; and

''(3) have such other related duties and authorities as may be assigned by the Secretary for purposes of the responsibilities described in paragraph (1), subject to the authority, direction, and control of the Secretary, in consultation with the Director of National Intelligence.

''(c) ASSISTANT SECRETARY FOR ECONOMIC INTELLIGENCE AND SECURITY.—The Office shall be headed by an Assistant Secretary, who shall be appointed by the President, by and with the advice and consent of the Senate. The Assistant Secretary shall report directly to the Undersecretary for Terrorism and Financial Crimes.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 3 of such title is amended by striking the item relating to section 311 and inserting the following:

''311. Office of Economic Intelligence and Security.''.

(c) CONFORMING AMENDMENT.—Section 3(4)(J) of the National Security Act of 1947 (50 U.S.C. 3003(4)(J))

is amended by striking ''Office of Intelligence and Analysis'' and inserting ''Office of Economic Intelligence and Security''.

(d) REFERENCES.—Any reference in a law, regulation, document, paper, or other record of the United States to the Office of Intelligence and Analysis of the Department of the Treasury shall be deemed a reference to the Office of Economic Intelligence and Security of the Department of the Treasury.

SEC. 313. REPORT ON SENSITIVE COMMERCIALLY AVAILABLE INFORMATION.

(a) DEFINITIONS.—

(1) COMMERCIALLY AVAILABLE INFORMATION.—The term ''commercially available information'' means—

(A) any data or other information of the type customarily made available or obtainable and sold, leased, or licensed to members of the general public or to non-governmental entities for purposes other than governmental purposes; or

(B) data and information for exclusive government use knowingly and voluntarily provided by, procured from, or made accessible by cor-

porate entities on their own initiative or at the request of a government entity.

(2) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means information that, alone or when combined with other information regarding an individual, can be used to distinguish or trace the identity of such individual.

(3) SENSITIVE ACTIVITIES.—The term ''sensitive activities'' means activities that, over an extended period of time—

(A) establish a pattern of life;

(B) reveal personal affiliations, preferences, or identifiers;

(C) facilitate prediction of future acts;

(D) enable targeting activities;

(E) reveal the exercise of individual rights and freedoms, including the rights to freedom of speech and of the press, to free exercise of religion, to peaceably assemble, including membership or participation in organizations or associations, and to petition the government; or

(F) reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the

United States person who engaged in the activity.

(4) SENSITIVE COMMERCIALLY AVAILABLE INFORMATION.—The term ''sensitive commercially available information''—

(A) means commercially available information that is known or reasonably expected to contain—

(i) a substantial volume of personally identifiable information regarding United States persons; or

(ii) a greater than de minims volume of sensitive data;

(B) shall not include—

(i) newspapers or other periodicals;

(ii) weather reports;

(iii) books;

(iv) journal articles or other published works;

(v) public filings or records;

(vi) documents or databases similar to those described in clauses (i) through (v), whether accessed through a subscription or accessible free of cost; or

(vii) limited data samples made available to elements of the intelligence community for the purposes of allowing such elements to determine whether to purchase the full dataset and not accessed, retained, or used for any other purpose.

(5) SENSITIVE DATA.—The term ''sensitive data'' means data that—

(A)(i) captures personal attributes, conditions, or identifiers that are traceable to 1 or more specific United States persons, either through the dataset or by correlating the dataset with other available information; and

(ii) concerns the race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data with respect to such specific United States person or United States persons the disclosure of which would have the potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the United States person or United States persons described by the data; or

(B) captures the sensitive activities of 1 or more United States persons.

(6) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an unorganized association substantially composed of United States citizens or permanent resident aliens; or

(C) an entity organized under the laws of the United States or of any jurisdiction within the United States, with the exception of any such entity directed or controlled by a foreign government.

(b) REPORT.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and annually thereafter, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on the access to, collection, processing, and use of sensitive commercially available information by the respective element.

(2) CONTENTS.—

(A) IN GENERAL.—For each dataset containing sensitive commercially available infor-

mation accessed, collected, processed, or used by the element concerned for purposes other than research and development, a report required by paragraph (1) shall include the following:

(i) A description of the nature and volume of the sensitive commercially available information accessed or collected by the element.

(ii) A description of the mission or administrative need or function for which the sensitive commercially available information is accessed or collected, and of the nature, scope, reliability, and timeliness of the dataset required to fulfill such mission or administrative need or function.

(iii) A description of the purpose of the access, collection, or processing, and the intended use of the sensitive commercially available information.

(iv) An identification of the legal authority for the collection or access, and processing of the sensitive commercially available information.

(v) An identification of the source of the sensitive commercially available information and the persons from whom the sensitive commercially available information was accessed or collected.

(vi) A description of the mechanics of the access, collection, and processing of the sensitive commercially available information, including the Federal entities that participated in the procurement process.

(vii) A description of the method by which the element has limited the access to and collection and processing of the sensitive commercially available information to the maximum extent feasible consistent with the need to fulfill the mission or administrative need.

(viii) An assessment of whether the mission or administrative need can be fulfilled if reasonably available privacy-enhancing techniques, such as filtering or anonymizing, the application of traditional safeguards, including access limitations and retention limits, differential privacy techniques, or other information-masking

techniques, such as restrictions or correlation, are implemented with respect to information concerning United States persons.

(ix) An assessment of the privacy and civil liberties risks associated with accessing, collecting, or processing the data and the methods by which the element mitigates such risks.

(x) An assessment of the applicability of section 552a of title 5, United States Code (commonly referred to as the ''Privacy Act of 1974''), if any.

(xi) To the extent feasible, an assessment of the original source of the data and the method through which the dataset was generated and aggregated, and whether any element of the intelligence community previously accessed or collected the same or similar sensitive commercially available information from the source.

(xii) An assessment of the quality and integrity of the data, including, as appropriate, whether the sensitive commercially available information reflects any under-

lying biases or inferences, and efforts to ensure that any intelligence products created with the data are consistent with the standards of the intelligence community for accuracy and objectivity.

(xiii) An assessment of the security, operational, and counterintelligence risks associated with the means of accessing or collecting the data, and recommendations for how the element could mitigate such risks.

(xiv) A description of the system in which the data is retained and processed and how the system is properly secured while allowing for effective implementation, management, and audit, as practicable, of relevant privacy and civil liberties protections.

(xv) An assessment of security risks posed by the system architecture of vendors providing sensitive commercially available information or access to such sensitive commercially available information, access restrictions for the data repository of each such vendor, and the vendor's access to

query terms and, if any, relevant safeguards.

(xvi) A description of procedures to restrict access to the sensitive commercially available information.

(xvii) A description of procedures for conducting, approving, documenting, and auditing queries, searches, or correlations with respect to the sensitive commercially available information.

(xviii) A description of procedures for restricting dissemination of the sensitive commercially available information, including deletion of information of United States persons returned in response to a query or other search unless the information is assessed to be associated or potentially associated with the documented mission-related justification for the query or search.

(xix) A description of masking and other privacy-enhancing techniques used by the element to protect sensitive commercially available information.

(xx) A description of any retention and deletion policies.

(xxi) A determination of whether unevaluated data or information has been made available to other elements of the intelligence community or foreign partners and, if so, identification of those elements or partners.

(xxii) A description of any licensing agreements or contract restrictions with respect to the sensitive commercially available information.

(xxiii) A data management plan for the lifecycle of the data, from access or collection to disposition.

(xxiv) For any item required by clauses (i) through (xxiii) that cannot be completed due to exigent circumstances relating to collecting, accessing, processing, or using sensitive commercially available information, a description of such exigent circumstances.

(B) RESEARCH AND DEVELOPMENT DATA.—For each dataset containing sensitive commercially available information accessed,

collected, processed, or used by the element concerned solely for research and development purposes, a report required by paragraph (1) may be limited to a description of the oversight by the element of such access, collection, process, and use.

(c) PUBLIC REPORT.—The Director of National Intelligence shall make available to the public, once every 2 years, a report on the policies and procedures of the intelligence community with respect to access to and collection, processing, and safeguarding of sensitive commercially available information.

SEC. 314. POLICY ON COLLECTION OF UNITED STATES LOCATION INFORMATION.

(a) DEFINITIONS.—In this section:

(1) UNITED STATES LOCATION INFORMATION.—The term ''United States location information'' means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, user, or device in the United States, or, if the customer, subscriber, or user is known to be a United States person, outside the United States.

(2) UNITED STATES PERSON.—The term ''United States person'' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Attorney General, shall issue a policy on the collection of United States location information by the intelligence community.

(c) CONTENT.—The policy required by subsection (a) shall address the filtering, segregation, use, dissemination, masking, and retention of United States location information.

(d) FORM; PUBLIC AVAILABILITY.—The policy required by subsection (a)—

(1) shall be issued in unclassified form and made available to the public; and

(2) may include a classified annex, which the Director of National Intelligence shall submit to the congressional intelligence committees.

SEC. 315. DISPLAY OF FLAGS, SEALS, AND EMBLEMS OTHER THAN THE UNITED STATES FLAG.

(a) DEFINITIONS.—In this section:

(1) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning given such term in section 105 of title 5, United States Code.

(2) NATIONAL INTELLIGENCE PROGRAM.—The term ''National Intelligence Program'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(b) IN GENERAL.—Any flag, seal, or emblem that is not the United States flag and is flown, draped, projected, or otherwise displayed as a visual and symbolic representation at a property, office, or other official location of an element of the intelligence community—

(1) shall be smaller than the official United States flag; and

(2) if flown, may not be displayed higher than or above the United States flag.

(c) LIMITATION ON AVAILABILITY OF FUNDS FOR DISPLAYING AND FLYING FLAGS.—None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2025 for the National Intelligence Program, may be obligated or expended to fly or display a flag over a facility of an element of the intelligence community other than the following:

(1) The United States flag.

(2) The POW/MIA flag.

(3) The Hostage and Wrongful Detainee flag, pursuant to section 904 of title 36, United States Code.

(4) The flag of a State, insular area, or the District of Columbia at a domestic location.

(5) The flag of an Indian Tribal Government.

(6) The official branded flag of an Executive agency.

(7) The flag of an element, flag officer, or general officer of the Armed Forces.

TITLE IV—COUNTERING FOREIGN THREATS

Subtitle A—People's Republic of China

SEC. 401. STRATEGY AND OUTREACH ON RISKS POSED BY PEOPLE'S REPUBLIC OF CHINA SMARTPORT TECHNOLOGY.

(a) STRATEGY AND OUTREACH REQUIRED.—The Director of the National Counterintelligence and Security Center shall develop a strategy and conduct outreach to United States industry, including shipping companies, port operators, and logistics firms, on the risks of smartport technology of the People's Republic of China and other related risks posed by entities of the People's Republic of China, including LOGINK, China Ocean Ship-

ping Company, Limited (COSCO), China Communications Construction Company, Limited (CCCC), China Media Group (CMG), and Shanghai Zhenhua Heavy Industries Company Limited (ZPMC), to the national security of the United States, the security of United States supply chains, and commercial activity, including with respect to delays, interruption, and lockout of access to systems and technologies that enable the free flow of commerce.

(b) CONSISTENCY WITH STATUTES AND EXECUTIVE ORDERS.—The Director shall carry out subsection (a) in a manner that is consistent with the following:

(1) Part 6 of title 33, Code of Federal Regulations, as amended by Executive Order 14116 (89 Fed. Reg. 13971; relating to amending regulations relating to the safeguarding of vessels, harbors, ports, and waterfront facilities of the United States.

(2) Executive Order 14017 (86 Fed. Reg. 11849; relating to America's supply chains), or successor order.

(3) Section 825 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31).

(c) COORDINATION.—The Director shall carry out subsection (a) in coordination with the Commandant of the Coast Guard, the Director of the Federal Bureau of

Investigation, the Commander of the Office of Naval Intelligence, and such other heads of Federal agencies as the Director considers appropriate.

SEC. 402. ASSESSMENT OF CURRENT STATUS OF BIOTECHNOLOGY OF PEOPLE'S REPUBLIC OF CHINA.

(a) ASSESSMENT.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the National Counterproliferation and Biosecurity Center and such heads of elements of the intelligence community as the Director of National Intelligence considers appropriate, conduct an assessment of the current status of the biotechnology of the People's Republic of China, which shall include an assessment of how the People's Republic of China is supporting the biotechnology sector through both licit and illicit means, such as foreign direct investment, subsidies, talent recruitment, or other efforts.

(b) REPORT.—

(1) IN GENERAL.—Not later than 30 days after the date on which the Direct of National Intelligence completes the assessment required by subsection (a), the Director shall submit to the congressional intelligence committees a report on the findings of the Director with respect to the assessment.

(2) FORM.—The report submitted pursuant to paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 403. INTELLIGENCE SHARING WITH LAW ENFORCEMENT AGENCIES ON SYNTHETIC OPIOID PRECURSOR CHEMICALS ORIGINATING IN PEOPLE'S REPUBLIC OF CHINA.

(a) STRATEGY REQUIRED.—The Director of National Intelligence shall, in consultation with the head of the Office of National Security Intelligence of the Drug Enforcement Administration, the Under Secretary of Homeland Security for Intelligence and Analysis, and the heads of such other agencies as the Director considers appropriate, develop a strategy to ensure robust intelligence sharing relating to the illicit trafficking of synthetic opioid precursor chemicals from the People's Republic of China and other source countries.

(b) MECHANISM FOR COLLABORATION.—The Director shall develop a mechanism so that subject matter experts in elements of the Federal Government other than elements in the intelligence community, including those without security clearances, can share information with the intelligence community relating to illicit trafficking described in subsection (a).

SEC. 404. REPORT ON EFFORTS OF THE PEOPLE'S REPUBLIC OF CHINA TO EVADE UNITED STATES TRANSPARENCY AND NATIONAL SECURITY REGULATIONS.

(a) REPORT REQUIRED.—The Director of National Intelligence shall submit to the congressional intelligence committees a report on efforts of the People's Republic of China to evade the following:

(1) Identification under section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 10 U.S.C. 113 note).

(2) Restrictions or limitations imposed by any of the following:

(A) Section 805 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31).

(B) Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 41 U.S.C. 3901 note prec.).

(C) The list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury (commonly known as the ''SDN list'').

(D) The Entity List maintained by the Bureau of Industry and Security of the Department of Commerce and set forth in Supplement No. 4 to part 744 of title 15, Code of Federal Regulations.

(E) Commercial or dual-use export controls under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) and the Export Administration Regulations.

(F) Executive Order 14105 (88 Fed. Reg. 54867; relating to addressing United States investments in certain national security technologies and products in countries of concern), or successor order.

(G) Import restrictions on products made with forced labor implemented by U.S. Customs and Border Protection pursuant to Public Law 117–78 (22 U.S.C. 6901 note).

(b) FORM.—The report submitted pursuant to subsection (a) shall be submitted in unclassified form.

SEC. 405. PLAN FOR RECRUITMENT OF MANDARIN SPEAKERS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate congressional

committees a comprehensive plan to prioritize the recruitment and training of individuals who speak Mandarin Chinese for each element of the intelligence community.

(b) APPROPRIATE CONGRESSIONAL COMMITTEES.—In this section, the term ''appropriate congressional committees'' means—

(1) the Select Committee on Intelligence and the Committee on the Judiciary of the Senate; and

(2) the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

Subtitle B—The Russian Federation

SEC. 411. ASSESSMENT OF RUSSIAN FEDERATION SPONSORSHIP OF ACTS OF INTERNATIONAL TERRORISM.

(a) DEFINITIONS.—In this section—

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Select Committee on Intelligence, the Committee on Foreign Relations, and the Committee on Armed Services of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, and the Committee on Armed Services of the House of Representatives.

(2) FOREIGN TERRORIST ORGANIZATION.—The term ''foreign terrorist organization'' means an organization that has been designated as a foreign terrorist organization by the Secretary of State, pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(3) SPECIALLY DESIGNATED GLOBAL TERRORIST ORGANIZATION.—The term ''specially designated global terrorist organization'' means an organization that has been designated as a specially designated global terrorist by the Secretary of State or the Secretary, pursuant to Executive Order 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).

(4) STATE SPONSOR OF TERRORISM.—The term ''state sponsor of terrorism'' means a country the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism, for purposes of—

(A) section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(c)(1)(A)(i));

(B) section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371);

(C) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or

(D) any other provision of law.

(b) ASSESSMENT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall conduct and submit to the appropriate congressional committees an assessment on the extent to which the Russian Federation—

(1) provides support for acts of international terrorism; and

(2) cooperates with the antiterrorism efforts of the United States.

(c) ELEMENTS.—The assessment required by subsection (b) shall include the following:

(1) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has failed to show support for or cooperate with the United States on international efforts to combat terrorism, such as apprehending, prosecuting, or extraditing suspected and known terrorists, including

members of foreign terrorist organizations, and sharing intelligence to deter terrorist attacks.

(2) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has provided financial, material, technical, or lethal support to foreign terrorist organizations, specially designated global terrorist organizations, state sponsors of terrorism, or for acts of international terrorism.

(3) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has willfully aided or abetted—

(A) the international proliferation of nuclear explosive devices to persons;

(B) a person in acquiring unsafeguarded special nuclear material; or

(C) the efforts of a person to use, develop, produce, stockpile, or otherwise acquire chemical, biological, or radiological weapons.

(4) A determination of whether the activities of the Wagner Group constitute acts of international terrorism and whether such activities continue under any of the successor entities of the Wagner Group, including Afrika Corps.

(d) FORM.—The assessment required by subsection (b) shall be submitted in unclassified form, but may include a classified annex.

(e) BRIEFINGS.—Not later than 30 days after submission of the assessment required by subsection (b), the Director of National Intelligence shall provide a classified briefing to the appropriate congressional committees on the methodology and findings of the assessment.

SEC. 412. ASSESSMENT OF LIKELY COURSE OF WAR IN UKRAINE.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in collaboration with the Director of the Defense Intelligence Agency and the Director of the Central Intelligence Agency, shall submit to the congressional intelligence committees an assessment of the likely course of the war in Ukraine through December 31, 2025.

(b) ELEMENTS.—The assessment required by subsection (a) shall include an assessment of each of the following:

(1) The ability of the military of Ukraine to defend against Russian aggression if the United States does, or does not, continue to provide military and economic assistance to Ukraine during the period described in such subsection.

(2) The likely course of the war during such period if the United States does, or does not, continue to provide military and economic assistance to Ukraine.

(3) The ability and willingness of countries in Europe and outside of Europe to continue to provide military and economic assistance to Ukraine if the United States does, or does not, do so, including the ability of such countries to make up for any shortfall in United States assistance.

(4) The effects of a potential defeat of Ukraine by the Russian Federation on the potential for further aggression from the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, and the Democratic People's Republic of Korea.

(c) FORM.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

Subtitle C—International Terrorism

SEC. 421. INCLUSION OF HAMAS, HEZBOLLAH, AL-QAEDA, AND ISIS OFFICIALS AND MEMBERS AMONG ALIENS ENGAGED IN TERRORIST ACTIVITY.

Section 212(a)(3)(B)(i) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)) is amended, in the undesignated matter following subparagraph (IX), by striking ''or spokesman of the Palestine Liberation Organization'' and inserting ''spokesperson, or member of the Palestine Liberation Organization, Hamas, Hezbollah, Al-Qaeda, ISIS, or any successor or affiliate group, or who endorses or espouses terrorist activities conducted by any of the aforementioned groups,''.

SEC. 422. ASSESSMENT AND REPORT ON THE THREAT OF ISIS-KHORASAN TO THE UNITED STATES.

(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Director of the National Counterterrorism Center, in coordination with such elements of the intelligence community as the Director considers relevant, shall—

(1) conduct an assessment of the threats to the United States and United States citizens posed by ISIS-Khorasan; and

(2) submit to the congressional intelligence committees a written report on the findings of the assessment.

(b) REPORT ELEMENTS.—The report required by subsection (a) shall include the following:

(1) A description of the historical evolution of ISIS-Khorasan, beginning with Al-Qaeda and the attacks on the United States on September 11, 2001.

(2) A description of the ideology and stated intentions of ISIS-Khorasan as related to the United States and the interests of the United States, including the homeland.

(3) A list of all terrorist attacks worldwide attributable to ISIS-Khorasan or for which ISIS-Khorasan claimed credit, beginning on January 1, 2015.

(4) A description of the involvement of ISIS-Khorasan in Afghanistan before, during, and after the withdrawal of United States military and civilian personnel and resources in August 2021.

(5) The recruiting and training strategy of ISIS-Khorasan following the withdrawal described in paragraph (4), including—

(A) the geographic regions in which ISIS-Khorasan is physically present;

(B) regions from which ISIS-Khorasan is recruiting; and

(C) its ambitions for individual actors worldwide and in the United States.

(6) A description of the relationship between ISIS-Khorasan and ISIS core, the Taliban, Al-Qaeda, and other terrorist groups, as appropriate.

(7) A description of the association of members of ISIS-Khorasan with individuals formerly detained at United States Naval Station, Guantanamo Bay, Cuba.

(8) A description of ISIS-Khorasan's development of, and relationships with, travel facilitation networks in Europe, Central Asia, Eurasia, and Latin America.

(9) An assessment of ISIS-Khorasan's understanding of the border and immigration policies and enforcement of the United States.

(10) An assessment of the known travel of members of ISIS-Khorasan within the Western Hemisphere and specifically across the southern border of the United States.

(c) FORM.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 423. TERRORIST FINANCING PREVENTION.

(a) DEFINITIONS.—In this section:

(1) DIGITAL ASSET.—The term ''digital asset'' means any digital representation of value that is recorded on a cryptographically secured distributed ledger or any similar technology, or another implementation which was designed and built as part of a system to leverage or replace blockchain or distributed ledger technology or their derivatives.

(2) DIGITAL ASSET PROTOCOL.—The term ''digital asset protocol'' means any communication protocol, smart contract, or other software—

(A) deployed through the use of distributed ledger or similar technology; and

(B) that provides a mechanism for users to interact and agree to the terms of a trade for digital assets.

(3) FOREIGN DIGITAL ASSET TRANSACTION FACILITATOR.—The term ''foreign digital asset transaction facilitator'' means any foreign person or group of foreign persons that, as determined by the Secretary, controls, operates, or makes available a digital asset protocol or similar facility, or otherwise materially assists in the purchase, sale, exchange, custody, or other transaction involving an exchange or transfer of value using digital assets.

(4) FOREIGN FINANCIAL INSTITUTION.—The term ''foreign financial institution'' has the meaning given that term under section 561.308 of title 31, Code of Federal Regulations.

(5) FOREIGN PERSON.—The term ''foreign person'' means an individual or entity that is not a United States person.

(6) FOREIGN TERRORIST ORGANIZATION.—The term ''foreign terrorist organization'' means an organization that has been designated as a foreign terrorist organization by the Secretary of State, pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(7) GOOD.—The term ''good'' means any article, natural or manmade substance, material, supply, or manufactured product, including inspection and test equipment, and excluding technical data.

(8) SECRETARY.—The term ''Secretary'' means the Secretary of the Treasury.

(9) SPECIALLY DESIGNATED GLOBAL TERRORIST ORGANIZATION.—The term ''specially designated global terrorist organization'' means an organization that has been designated as a specially designated global terrorist by the Secretary of State or the Secretary, pursuant to Executive Order

13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).

(10) UNITED STATES PERSON.—The term ''United States person'' means—

(A) an individual who is a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person in the United States.

(b) SANCTIONS WITH RESPECT TO FOREIGN FINANCIAL INSTITUTIONS AND FOREIGN DIGITAL ASSET TRANSACTION FACILITATORS THAT ENGAGE IN CERTAIN TRANSACTIONS.—

(1) MANDATORY IDENTIFICATION.—Not later than 60 days after the date of enactment of this Act, and periodically thereafter, the Secretary shall identify and submit to the President a report identifying any foreign financial institution or foreign digital asset transaction facilitator that has knowingly—

(A) facilitated a significant financial transaction with—

(i) a Foreign Terrorist Organization;

(ii) a specially designated global terrorist organization; or

(iii) a person identified on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) for acting on behalf of or at the direction of, or being owned or controlled by, a foreign terrorist organization or a specially designated global terrorist organization; or

(B) engaged in money laundering to carry out an activity described in subparagraph (A).

(2) IMPOSITION OF SANCTIONS.—

(A) FOREIGN FINANCIAL INSTITUTIONS.—The President shall prohibit, or impose strict conditions on, the opening or maintaining of a correspondent account or a payable-through ac-

count in the United States by a foreign financial institution identified under paragraph (1).

(B) FOREIGN DIGITAL ASSET TRANSACTION FACILITATORS.—The President, pursuant to such regulations as the President may prescribe, shall prohibit any transactions between any person subject to the jurisdiction of the United States and a foreign digital asset transaction facilitator identified under paragraph (1).

(3) IMPLEMENTATION AND PENALTIES.—

(A) IMPLEMENTATION.—The President may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702, 1704) to the extent necessary to carry out this Act.

(B) PENALTIES.—The penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) shall apply to a person that violates, attempts to violate, conspires to violate, or causes a violation of regulations prescribed under this section to the same extent that such penalties apply to a person that com-

mits an unlawful act described in subsection (a) of such section 206.

(4) PROCEDURES FOR JUDICIAL REVIEW OF CLASSIFIED INFORMATION.—

(A) IN GENERAL.—If a finding under this subsection, or a prohibition, condition, or penalty imposed as a result of any such finding, is based on classified information (as defined in section 1(a) of the Classified Information Procedures Act (18 U.S.C. App.)), the Secretary may submit to a court reviewing the finding or the imposition of the prohibition, condition, or penalty such classified information ex parte and in camera.

(B) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to confer or imply any right to judicial review of any finding under this subsection or any prohibition, condition, or penalty imposed as a result of any such finding.

(5) WAIVER FOR NATIONAL SECURITY.—The Secretary may waive the imposition of sanctions under this subsection with respect to a person if the Secretary—

(A) determines that such a waiver is in the national interests of the United States; and

(B) submits to Congress a notification of the waiver and the reasons for the waiver.

(6) EXCEPTION FOR INTELLIGENCE ACTIVITIES.—This subsection shall not apply with respect to any activity subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) or any authorized intelligence activities of the United States.

(7) EXCEPTION RELATING TO IMPORTATION OF GOODS.—The authorities and requirements under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(c) SPECIAL MEASURES FOR MODERN THREATS.—Section 5318A of title 31, United States Code, is amended—

(1) in subsection (a)(2)(C), by striking ''subsection (b)(5)'' and inserting ''paragraphs (5) and (6) of subsection (b)''; and

(2) in subsection (b)—

(A) in paragraph (5), by striking ''for or on behalf of a foreign banking institution''; and

(B) by adding at the end the following:

"(6) PROHIBITIONS OR CONDITIONS ON CERTAIN TRANSMITTALS OF FUNDS.—If the Secretary finds a jurisdiction outside of the United States, 1 or more financial institutions operating outside of the United States, 1 or more types of accounts within, or involving, a jurisdiction outside of the United States, or 1 or more classes of transactions within, or involving, a jurisdiction outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the Secretary of State, the Attorney General, and the Chairman of the Board of Governors of the Federal Reserve System, may prohibit, or impose conditions upon, certain transmittals of funds (as such term may be defined by the Secretary in a special measure issuance, by regulation, or as otherwise permitted by law), to or from any domestic financial institution or domestic financial agency if such transmittal of funds involves any such jurisdiction, institution, type of account, class of transaction, or type of account.".

(d) FUNDING.—There is authorized to be appropriated to the Secretary such funds as are necessary to carry out the purposes of this section.

Subtitle D—Other Foreign Threats

SEC. 431. ASSESSMENT OF VISA-FREE TRAVEL TO AND WITHIN WESTERN HEMISPHERE BY NATIONALS OF COUNTRIES OF CONCERN.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a written assessment of the impacts to national security caused by travel without a visa to and within countries in the Western Hemisphere by nationals of countries of concern.

(b) FORM.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) COUNTRIES OF CONCERN DEFINED.—In this section, the term ''countries of concern'' means—

(1) the Russian Federation;

(2) the People's Republic of China;

(3) the Islamic Republic of Iran;

(4) the Syrian Arab Republic;

(5) the Democratic People's Republic of Korea;

(6) the Bolivarian Republic of Venezuela; and

(7) the Republic of Cuba.

SEC. 432. STUDY ON THREAT POSED BY FOREIGN INVESTMENT IN UNITED STATES AGRICULTURAL LAND.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Select Committee on Intelligence, the Committee on Agriculture, Nutrition, and Forestry, the Committee on Foreign Relations, and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Agriculture, the Committee on Foreign Affairs, and the Committee on Financial Services of the House of Representatives.

(2) DIRECTOR.—The term ''Director'' means the Director of National Intelligence.

(3) NONMARKET ECONOMY COUNTRY.—The term ''nonmarket economy country'' has the meaning given that term in section 771(18) of the Tariff Act of 1930 (19 U.S.C. 1677(18)).

(b) STUDY AND BRIEFING.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Director,

in coordination with the elements of the intelligence community the Director considers appropriate and with the Secretary of State, the Secretary of Agriculture, and the Secretary of the Treasury, shall—

(A) complete a study on the threat posed to the United States by foreign investment in agricultural land in the United States; and

(B) provide to the appropriate committees of Congress a briefing on the results of the study.

(2) DATA.—In conducting the study required by paragraph (1), the Director shall process and analyze relevant data collected by the Secretary of State, the Secretary of Agriculture, and the Secretary of the Treasury, including the information submitted to the Secretary of Agriculture under section 2 of the Agricultural Foreign Investment Disclosure Act of 1978 (7 U.S.C. 3501).

(3) ELEMENTS.—The study required by paragraph (1) shall include the following:

(A) Data and an analysis of agricultural land holdings, including current and previous uses of the land disaggregated by sector and industry, in each county in the United States held by a foreign person from—

(i) a country identified as a country that poses a risk to the national security of the United States in the most recent annual report on worldwide threats issued by the Director pursuant to section 108B of the National Security Act of 1947 (50 U.S.C. 3043b) (commonly known as the ''Annual Threat Assessment'');

(ii) a nonmarket economy country; or

(iii) any other country that the Director determines to be appropriate.

(B) An analysis of the proximity of the agricultural land holdings to critical infrastructure and military installations.

(C) An assessment of the threats posed to the national security of the United States by malign actors that use foreign investment in agricultural land in the United States.

(D) An assessment of warning indicators and methods by which to detect potential threats from the use by foreign adversaries of agricultural products for nefarious ends.

(E) An assessment of additional resources or authorities necessary to counter threats identified during the study.

SEC. 433. ASSESSMENT OF THREAT POSED BY CITIZENSHIP-BY-INVESTMENT PROGRAMS.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Homeland Security, the Committee on Foreign Affairs, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(2) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury.

(3) CITIZENSHIP-BY-INVESTMENT PROGRAM.—The term ''citizenship-by-investment program'' means an immigration, investment, or other program of a foreign country that, in exchange for a

covered contribution, authorizes the individual making the covered contribution to acquire citizenship in such country, including temporary or permanent residence that may serve as the basis for subsequent naturalization.

(4) COVERED CONTRIBUTION.—The term ''covered contribution'' means—

(A) an investment in, or a monetary donation or any other form of direct or indirect capital transfer to, including through the purchase or rental of real estate—

(i) the government of a foreign country; or

(ii) any person, business, or entity in such a foreign country; and

(B) a donation to, or endowment of, any activity contributing to the public good in such a foreign country.

(5) DIRECTOR.—The term ''Director'' means the Director of National Intelligence.

(b) ASSESSMENT OF THREAT POSED BY CITIZENSHIP-BY-INVESTMENT PROGRAMS.—

(1) ASSESSMENT.—Not later than 1 year after the date of the enactment of this Act, the Director and the Assistant Secretary, in coordination with the

heads of the other elements of the intelligence community and the head of any appropriate Federal agency, shall complete an assessment of the threat posed to the United States by citizenship-by-investment programs.

(2) ELEMENTS.—The assessment required by paragraph (1) shall include the following:

(A) An identification of each citizenship-by-investment program, including an identification of the foreign country that operates each such program.

(B) With respect to each citizenship-by-investment program identified under subparagraph (A)—

(i) a description of the types of investments required under the program; and

(ii) an identification of the sectors to which an individual may make a covered contribution under the program.

(C) An assessment of the threats posed to the national security of the United States by malign actors that use citizenship-by-investment programs—

(i) to evade sanctions or taxes;

(ii) to facilitate or finance—

(I) crimes relating to national security, including terrorism, weapons trafficking or proliferation, cybercrime, drug trafficking, human trafficking, and espionage; or

(II) any other activity that furthers the interests of a foreign adversary or undermines the integrity of the immigration laws or security of the United States; or

(iii) to undermine the United States and its interests through any other means identified by the Director and the Assistant Secretary.

(D) An identification of the foreign countries the citizenship-by-investment programs of which pose the greatest threat to the national security of the United States.

(3) REPORT AND BRIEFING.—

(A) REPORT.—

(i) IN GENERAL.—Not later than 180 days after completing the assessment required by paragraph (1), the Director and the Assistant Secretary shall jointly submit to the appropriate committees of Congress

a report on the findings of the Director and the Assistant Secretary with respect to the assessment.

(ii) ELEMENTS.—The report required by clause (i) shall include the following:

(I) A detailed description of the threats posed to the national security of the United States by citizenship-by-investment programs.

(II) Recommendations for additional resources or authorities necessary to counter such threats.

(III) A description of opportunities to counter such threats.

(iii) FORM.—The report required by clause (i) shall be submitted in unclassified form but may include a classified annex, as appropriate.

(B) BRIEFING.—Not later than 90 days after the date on which the report required by subparagraph (A) is submitted, the Director and Assistant Secretary shall provide the appropriate committees of Congress with a briefing on the report.

SEC. 434. MITIGATING THE USE OF UNITED STATES COMPONENTS AND TECHNOLOGY IN HOSTILE ACTIVITIES BY FOREIGN ADVERSARIES.

(a) FINDINGS.—Congress finds the following:

(1) Foreign defense material, including advanced military and intelligence capabilities, continues to rely heavily on products and services sourced from the United States.

(2) Iran drones operating against Ukraine were found to include several United States components.

(3) The components described in paragraph (2) came from 13 different United States companies and are integral to the operation of the drones.

(4) The Chinese spy balloon that flew across the United States in 2023 used a United States internet service provider to communicate.

(5) The connection allowed the balloon to send burst transmissions, or high-bandwidth collections of data over short periods.

(6) Foreign adversaries and affiliated foreign defense companies frequently acquire components and services, sourced from the United States, through violation of United States export control laws.

(b) SUPPLY CHAIN RISK MITIGATION.—Not later than 180 days after the date of the enactment of this Act,

the Director of National Intelligence shall, in collaboration with such heads of elements of the intelligence community as the Director considers appropriate, develop and commence implementation of a strategy to work with United States companies to mitigate or disrupt the acquisition and use of United States components in the conduct of activities harmful to the national security of the United States.

(c) GOAL.—The goal of the strategy required by subsection (b) shall be to inform and provide intelligence support to government and private sector entities in preventing United States components and technologies from aiding or supporting hostile or harmful activities conducted by foreign adversaries of the United States.

(d) CONSULTATION.—In developing and implementing the strategy required by subsection (b), the Director of National Intelligence—

(1) shall consult with the Secretary of Commerce, the Secretary of Defense, and the Secretary of Homeland Security; and

(2) may consult with such other heads of Federal departments or agencies as the Director of National Intelligence considers appropriate.

(e) ANNUAL REPORTS.—Not later than 1 year after the date of the enactment of this Act and annually there-

after until the date that is 3 years after the date of the enactment of this Act, the Director shall submit to Congress an annual report on the status and effect of the implementation of the strategy required by subsection (b).

SEC. 435. OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE REVIEW OF VISITORS AND ASSIGNEES.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Select Committee on Intelligence and the Committee on Energy and Natural Resources of the Senate; and

(B) the Permanent Select Committee on Intelligence and the Committee on Energy and Commerce of the House of Representatives.

(2) ASSIGNEE; VISITOR.—The terms ''assignee'' and ''visitor'' mean a foreign national from a country identified in the report submitted to Congress by the Director of National Intelligence in 2024 pursuant to section 108B of the National Security Act of 1947 (50 U.S.C. 3043b) (commonly referred to as the ''Annual Threat Assessment'') as ''engaging in competitive behavior that directly threatens U.S. na-

tional security'', who is not an employee of a National Laboratory, and has requested access to the premises, information, or technology of a National Laboratory.

(3) DIRECTOR.—The term ''Director'' means the Director of the Office of Intelligence and Counterintelligence of the Department of Energy (or their designee).

(4) FOREIGN NATIONAL.—The term ''foreign national'' has the meaning given the term ''alien'' in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(5) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(6) NON-TRADITIONAL COLLECTOR.—The term ''non-traditional collector'' means an individual not employed by a foreign intelligence service, who is seeking access to sensitive information about a capability, research, or organizational dynamics of the United States to inform a foreign adversary or non-state actor.

(b) FINDINGS.—The Senate finds the following:

(1) The National Laboratories conduct critical, cutting-edge research across a range of scientific disciplines that provide the United States with a technological edge over other countries.

(2) The technologies developed in the National Laboratories contribute to the national security of the United States, including classified and sensitive military technology and dual-use commercial technology.

(3) International cooperation in the field of science is critical to the United States maintaining its leading technological edge.

(4) The research enterprise of the Department of Energy, including the National Laboratories, is increasingly targeted by adversarial nations to exploit military and dual-use technologies for military or economic gain.

(5) Approximately 40,000 citizens of foreign countries, including more than 8,000 citizens from China and Russia, were granted access to the premises, information, or technology of National Laboratories in fiscal year 2023.

(6) The Office of Intelligence and Counterintelligence of the Department of Energy is responsible for identifying and mitigating counterintelligence

risks to the Department, including the National Laboratories.

(c) SENSE OF THE SENATE.—It is the sense of the Senate that, before being granted access to the premises, information, or technology of a National Laboratory, citizens of foreign countries identified in the 2024 Annual Threat Assessment of the intelligence community as ''engaging in competitive behavior that directly threatens U.S. national security'' should be appropriately screened by the National Laboratory to which they seek access, and by the Office of Intelligence and Counterintelligence of the Department, to identify and mitigate risks associated with granting the requested access to sensitive military, or dual-use technologies.

(d) REVIEW OF SENSITIVE COUNTRY VISITOR AND ASSIGNEE ACCESS REQUESTS.—The Director shall promulgate a policy to assess the counterintelligence risk each visitor or assignee poses to the research or activities undertaken at a National Laboratory.

(e) ADVICE WITH RESPECT TO VISITORS OR ASSIGNEES.—

(1) IN GENERAL.—The Director shall provide advice to a National Laboratory on visitors and assignees when 1 or more of the following conditions are present:

(A) The Director has reason to believe that a visitor or assignee is a non-traditional intelligence collector.

(B) The Director is in receipt of information indicating that a visitor or assignee constitutes a counterintelligence risk to a National Laboratory.

(2) ADVICE DESCRIBED.—Advice provided to a National Laboratory in accordance with paragraph (1) shall include—

(A) a description of the assessed risk;

(B) recommendations to mitigate the risk; and

(C) identification of research or technology that would be at risk if access is granted to the visitor or assignee concerned.

(f) REPORTS TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, and quarterly thereafter, the Director shall submit to the appropriate congressional committees a report, which shall include—

(1) the number of visitors or assignees permitted to access the premises, information, or technology of each National Laboratory;

(2) the number of instances in which the Director advised a National Laboratory in accordance with subsection (e); and

(3) the number of instances in which a National Laboratory admitted a visitor or assignee against the advice of the Director.

SEC. 436. PROHIBITION ON NATIONAL LABORATORIES ADMITTING CERTAIN FOREIGN NATIONALS.

(a) DEFINITIONS.—In this section:

(1) ASSIGNEE.—The term ''assignee'' means an individual who is seeking approval from, or has been approved by, a National Laboratory to access the premises, information, or technology of the National Laboratory for a period of more than 30 consecutive days.

(2) COVERED FOREIGN NATIONAL.—

(A) IN GENERAL.—The term ''covered foreign national'' means a foreign national of any of the following countries:

(i) The People's Republic of China.

(ii) The Russian Federation.

(iii) The Islamic Republic of Iran.

(iv) The Democratic People's Republic of Korea.

(v) The Republic of Cuba.

(B) EXCLUSION.—The term ''covered foreign national'' does not include an individual that is lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

(3) FOREIGN NATIONAL.—The term ''foreign national'' has the meaning given the term ''alien'' in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(4) NATIONAL LABORATORY.—The term ''National Laboratory'' has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(5) SENIOR COUNTERINTELLIGENCE OFFICIAL.—The term ''senior counterintelligence official'' means—

(A) the Director of the Federal Bureau of Investigation;

(B) the Deputy Director of the Federal Bureau of Investigation;

(C) the Executive Assistant Director of the National Security Branch of the Federal Bureau of Investigation; or

(D) the Assistant Director of the Counterintelligence Division of the Federal Bureau of Investigation.

(6) VISITOR.—The term ''visitor'' means an individual who is seeking approval from, or has been approved by, a National Laboratory to access the premises, information, or technology of the National Laboratory for any period shorter than a period described in paragraph (1).

(b) PROHIBITION.—

(1) IN GENERAL.—Except as provided in paragraph (2), beginning on the date of enactment of this Act, a National Laboratory—

(A) shall not admit as a visitor or assignee any covered foreign national; and

(B) shall prohibit access to any visitor or assignee that is a covered foreign national and has sought or obtained approval to access the premises, information, or technology of the National Laboratory as of that date.

(2) WAIVER.—Paragraph (1) shall not apply to a National Laboratory if the Secretary of Energy, in consultation with the Director of the Office of Intelligence and Counterintelligence of the Department of Energy and a senior counterintelligence official, cer-

tifies and issues a waiver to the National Laboratory requesting to admit a covered foreign national as a visitor or assignee, in writing, that the benefits to the United States of admittance or access by that covered foreign national outweigh the national security and economic risks to the United States.

(3) NOTIFICATION TO CONGRESS.—Not later than 30 days after the date that a waiver is issued pursuant to paragraph (2), the Secretary of Energy shall submit to the Select Committee on Intelligence of the Senate, the Committee on Energy and Natural Resources of the Senate, the Committee on Commerce, Science, and Transportation of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on Energy and Commerce of the House of Representatives, and the Committee on Science, Space, and Technology of the House of Representatives a notification describing each waiver issued pursuant to paragraph (2), including—

(A) the country of origin of the covered foreign national who is the subject of the waiver;

(B) the date of the request by the covered foreign national for admission or access to a National Laboratory;

(C) the date on which the decision to issue the waiver was made; and

(D) the specific reasons for issuing the waiver.

SEC. 437. QUARTERLY REPORT ON CERTAIN FOREIGN NATIONALS ENCOUNTERED AT THE UNITED STATES BORDER.

(a) DEFINITIONS.—In this section:

(1) ENCOUNTERED.—The term ''encountered'', with respect to a special interest alien, means physically apprehended by U.S. Customs and Border Protection personnel.

(2) SPECIAL INTEREST ALIEN.—The term ''special interest alien'' means an alien (as defined in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)) who, based upon an analysis of travel patterns and other information available to the United States Government, potentially poses a threat to the national security of the United States and its interests due to a known or potential nexus to terrorism, espionage, organized crime, or other malign actors.

(b) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and quarterly thereafter for the following 3 years, the Secretary of Homeland Security, in coordination with the Director of National Intelligence, shall publish, on a publicly accessible website of the Department of Homeland Security, a report identifying the aggregate number of special interest aliens who, during the applicable reporting period—

(1) have been encountered at or near an international border of the United States; and

(2)(A) have been released from custody;

(B) are under supervision;

(C) are being detained by the Department of Homeland Security; or

(D) have been removed from the United States.

SEC. 438. ASSESSMENT OF THE LESSONS LEARNED BY THE INTELLIGENCE COMMUNITY WITH RESPECT TO THE ISRAEL-HAMAS WAR.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with such other heads of elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress a written assessment of the lessons learned from the Israel-Hamas war.

(b) ELEMENTS.—The assessment required by subsection (a) shall include the following:

(1) Lessons learned from the timing and scope of the October 7, 2023 attack by Hamas against Israel, including lessons related to United States intelligence cooperation with Israel and other regional partners.

(2) Lessons learned from advances in warfare, including the use by adversaries of a complex tunnel network.

(3) Lessons learned from attacks by adversaries against maritime shipping routes in the Red Sea.

(4) Lessons learned from the use by adversaries of rockets, missiles, and unmanned aerial systems, including attacks by Iran.

(5) Analysis of the impact of the Israel-Hamas war on the global security environment, including the war in Ukraine.

(c) FORM.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

SEC. 439. CENTRAL INTELLIGENCE AGENCY INTELLIGENCE ASSESSMENT ON TREN DE ARAGUA.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency, in consultation with such other heads of elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress an intelligence assessment on the gang known as ''Tren de Aragua''.

(b) ELEMENTS.—The intelligence assessment required by subsection (a) shall include the following:

(1) A description of the key leaders, organizational structure, subgroups, presence in countries in the Western Hemisphere, and cross-border illicit drug smuggling routes of Tren de Aragua.

(2) A description of the practices used by Tren de Aragua to generate revenue.

(3) A description of the level at which Tren de Aragua receives support from the regime of Nicolás Maduro in Venezuela.

(4) A description of the manner in which Tren de Aragua is exploiting heightened migratory flows out of Venezuela and throughout the Western Hemisphere to expand its operations.

(5) A description of the degree to which Tren de Aragua cooperates or competes with other criminal organizations in the Western Hemisphere.

(6) An estimate of the annual revenue received by Tren de Aragua from the sale of illicit drugs, kidnapping, and human trafficking, disaggregated by activity.

(7) A determination on whether Tren De Aragua meets the definition of ''significant transnational criminal organization'' in section 3 of Executive Order 13581 (76 Fed. Reg. 44757; relating to blocking property of transnational criminal organizations), as amended by Executive Order 13863 (84 Fed. Reg. 10255; relating to taking additional steps to address the national emergency with respect to significant transnational criminal organizations).

(8) Any other information the Director of the Central Intelligence Agency considers relevant.

(c) FORM.—The intelligence assessment required by subsection (a) may be submitted in classified form.

(d) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this section, the term ''appropriate committees of Congress'' means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Appropriations of the Senate; and

(3) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

SEC. 440. ASSESSMENT OF MADURO REGIME'S ECONOMIC AND SECURITY RELATIONSHIPS WITH STATE SPONSORS OF TERRORISM AND FOREIGN TERRORIST ORGANIZATIONS.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a written assessment of the economic and security relationships of the regime of Nicolás Maduro of Venezuela with the countries and organizations described in subsection (b), including formal and informal support to and from such countries and organizations.

(b) COUNTRIES AND ORGANIZATIONS DESCRIBED.—The countries and organizations described in this subsection are the following:

(1) The following countries designated by the United States as state sponsors of terrorism:

(A) The Republic of Cuba.

(B) The Islamic Republic of Iran.

(2) The following organizations designated by the United States as foreign terrorist organizations:

(A) The National Liberation Army (ELN).

(B) The Revolutionary Armed Forces of Colombia–People's Army (FARC-EP).

(C) The Segunda Marquetalia.

(c) FORM.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 441. CONTINUED CONGRESSIONAL OVERSIGHT OF IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.

(a) UPDATE REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees an update to the report submitted under section 6705 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for

Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) to reflect current occurrences, circumstances, and expenditures.

(b) FORM.—The update submitted pursuant to subsection (a) shall be submitted in unclassified form, but may include a classified annex.

TITLE V—EMERGING TECHNOLOGIES

SEC. 501. STRATEGY TO COUNTER FOREIGN ADVERSARY EFFORTS TO UTILIZE BIOTECHNOLOGIES IN WAYS THAT THREATEN UNITED STATES NATIONAL SECURITY.

(a) SENSE OF CONGRESS.—It is the sense of Congress that as biotechnologies become increasingly important with regard to the national security interests of the United States, and with the addition of biotechnologies to the biosecurity mission of the National Counterproliferation and Biosecurity Center, the intelligence community must articulate and implement a whole-of-government strategy for addressing concerns relating to biotechnologies.

(b) STRATEGY FOR BIOTECHNOLOGIES CRITICAL TO NATIONAL SECURITY.—

(1) STRATEGY REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the

Director of National Intelligence shall, acting through the Director of the National Counterproliferation and Biosecurity Center and in coordination with the heads of such other elements of the intelligence community as the Director of National Intelligence considers appropriate, develop and submit to the congressional intelligence committees a whole-of-government strategy to address concerns relating to biotechnologies.

(2) ELEMENTS.—The strategy developed and submitted pursuant to paragraph (1) shall include the following:

(A) Identification and assessment of biotechnologies critical to the national security of the United States, including an assessment of which materials involve a dependency on foreign adversary nations.

(B) A determination of how best to counter foreign adversary efforts to utilize biotechnologies that threaten the national security of the United States, including technologies identified pursuant to paragraph (1).

(C) A plan to support United States efforts and capabilities to secure the United States supply chains of the technologies identi-

fied pursuant to paragraph (1), by coordinating—

(i) across the intelligence community;

(ii) the support provided by the intelligence community to other relevant Federal agencies and policymakers;

(iii) the engagement of the intelligence community with private sector entities; and

(iv) how the intelligence community can support securing United States supply chains for and use of biotechnologies.

(D) Proposals for such legislative or administrative action as the Directors consider necessary to support the strategy.

SEC. 502. IMPROVEMENTS TO THE ROLES, MISSIONS, AND OBJECTIVES OF THE NATIONAL COUNTERPROLIFERATION AND BIOSECURITY CENTER.

Section 119A of the National Security Act of 1947 (50 U.S.C. 3057) is amended—

(1) in subsection (a)(4), by striking ''biosecurity and'' and inserting ''counterproliferation, biosecurity, and''; and

(2) in subsection (b)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking ''analyzing and'';

(ii) in subparagraph (C), by striking ''Establishing'' and inserting ''Coordinating the establishment of'';

(iii) in subparagraph (D), by striking ''Disseminating'' and inserting ''Overseeing the dissemination of'';

(iv) in subparagraph (E), by inserting ''and coordinating'' after ''Conducting''; and

(v) in subparagraph (G), by striking ''Conducting'' and inserting ''Coordinating and advancing''; and

(B) in paragraph (2)—

(i) in subparagraph (B), by striking ''and analysis'';

(ii) by redesignating subparagraphs (C) through (E) as subparagraphs (D) through (F), respectively;

(iii) by inserting after subparagraph (B) the following:

''(C) Overseeing and coordinating the analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence

needs of Federal departments and agencies responsible for public health, including by providing analytic priorities to elements of the intelligence community and by conducting and coordinating net assessments.'';

(iv) in subparagraph (D), as redesignated by clause (ii), by inserting ''on matters relating to biosecurity and foreign biological threats'' after ''public health'';

(v) in subparagraph (F), as redesignated by clause (ii), by inserting ''and authorities'' after ''capabilities''; and

(vi) by adding at the end the following:

''(G) Coordinating with relevant elements of the intelligence community and other Federal departments and agencies responsible for public health to engage with private sector entities on information relevant to biosecurity, biotechnology, and foreign biological threats.''.

SEC. 503. ENHANCING CAPABILITIES TO DETECT FOREIGN ADVERSARY THREATS RELATING TO BIOLOGICAL DATA.

Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence

shall, in consultation with the heads of such Federal departments and agencies as the Director considers appropriate, take the following steps to standardize and enhance the capabilities of the intelligence community to detect foreign adversary threats relating to biological data:

(1) Prioritize the collection, analysis, and dissemination of information relating to foreign adversary use of biological data, particularly in ways that threaten or could threaten the national security of the United States.

(2) Issue policy guidance within the intelligence community—

(A) to standardize the handling and processing of biological data, including with respect to protecting the civil liberties and privacy of United States persons;

(B) to standardize and enhance intelligence engagements with foreign allies and partners with respect to biological data; and

(C) to standardize the creation of metadata relating to biological data.

(3) Ensure coordination with such Federal departments and agencies and entities in the private sector as the Director considers appropriate to understand how foreign adversaries are accessing and

using biological data stored within the United States.

SEC. 504. NATIONAL SECURITY PROCEDURES TO ADDRESS CERTAIN RISKS AND THREATS RELATING TO ARTIFICIAL INTELLIGENCE.

(a) FINDINGS.—Congress finds the following:

(1) Artificial intelligence systems demonstrate increased capabilities in the generation of synthetic media and computer programming code, as well as areas such as object recognition, natural language processing, and workflow orchestration.

(2) The growing capabilities of artificial intelligence systems in the areas described in paragraph (1), as well as the greater accessibility of large-scale artificial intelligence models and advanced computation capabilities to individuals, businesses, and governments, have dramatically increased the adoption of artificial intelligence products in the United States and globally.

(3) The advanced capabilities of the systems described in paragraph (1), and their accessibility to a wide-range of users, have increased the likelihood and effect of misuse or malfunction of these systems, such as to generate synthetic media for disinformation campaigns, develop or refine malware

for computer network exploitation activity, enhance surveillance capabilities in ways that undermine the privacy of citizens of the United States, and increase the risk of exploitation or malfunction of information technology systems incorporating artificial intelligence systems in mission-critical fields such as health care, critical infrastructure, and transportation.

(b) PROCEDURES REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the President shall develop and issue procedures to facilitate and promote mechanisms by which—

(1) vendors of advanced computation capabilities, vendors and commercial users of artificial intelligence systems, as well as independent researchers and other third parties, may effectively notify appropriate elements of the United States Government of—

(A) information security risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system to develop or refine malicious software;

(B) information security risks such as indications of compromise or other threat information indicating a compromise to the confiden-

tiality, integrity, or availability of an artificial intelligence system, or to the supply chain of an artificial intelligence system, including training or test data, frameworks, computing environments, or other components necessary for the training, management, or maintenance of an artificial intelligence system;

(C) biosecurity risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system to design, develop, or acquire dual-use biological entities such as putatively toxic small molecules, proteins, or pathogenic organisms;

(D) suspected foreign malign influence (as defined by section 119C of the National Security Act of 1947 (50 U.S.C. 3059(f))) activity that appears to be facilitated by an artificial intelligence system; and

(E) any other unlawful activity facilitated by, or directed at, an artificial intelligence system;

(2) elements of the Federal Government may provide threat briefings to vendors of advanced computation capabilities and vendors of artificial intelligence systems, alerting them, as may be appro-

priate, to potential or confirmed foreign exploitation of their systems, as well as malign foreign plans and intentions.

(c) BRIEFING REQUIRED.—

(1) APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the congressional intelligence committees;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) IN GENERAL.—The President shall provide the appropriate committees of Congress a briefing on procedures developed and issued pursuant to subsection (b).

(3) ELEMENTS.—The briefing provided pursuant to paragraph (2) shall include the following:

(A) A clear specification of which Federal agencies are responsible for leading outreach to affected industry and the public with respect to the matters described in subparagraphs (A) through (E) of paragraph (1) of subsection (b) and paragraph (2) of such subsection.

(B) An outline of a plan for industry outreach and public education regarding risks posed by, and directed at, artificial intelligence systems.

(C) Use of research and development, stakeholder outreach, and risk management frameworks established pursuant to—

(i) provisions of law in effect on the day before the date of the enactment of this Act; or

(ii) Federal agency guidelines.

SEC. 505. ESTABLISHMENT OF ARTIFICIAL INTELLIGENCE SECURITY CENTER.

(a) ESTABLISHMENT.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Security Agency shall establish an Artificial Intelligence Security Center within the Cybersecurity Collaboration Center of the National Security Agency.

(b) FUNCTIONS.—The functions of the Artificial Intelligence Security Center shall be as follows:

(1) Making available a research test bed to private sector and academic researchers, on a subsidized basis, to engage in artificial intelligence security research, including through the secure provision of access in a secure environment to proprietary

third-party models, with the consent of the vendors of the models.

(2) Developing guidance to prevent or mitigate counter-artificial intelligence techniques.

(3) Promoting secure artificial intelligence adoption practices for managers of national security systems (as defined in section 3552 of title 44, United States Code) and elements of the defense industrial base.

(4) Coordinating with the Artificial Intelligence Safety Institute of the National Institute of Standards and Technology.

(5) Such other functions as the Director considers appropriate.

(c) TEST BED REQUIREMENTS.—

(1) ACCESS AND TERMS OF USAGE.—

(A) RESEARCHER ACCESS.—The Director shall establish terms of usage governing researcher access to the test bed made available under subsection (b)(1), with limitations on researcher publication only to the extent necessary to protect classified information or proprietary information concerning third-party models provided through the consent of model vendors.

(B) AVAILABILITY TO FEDERAL AGENCIES.—The Director shall ensure that the test bed made available under subsection (b)(1) is also made available to other Federal agencies on a cost-recovery basis.

(2) USE OF CERTAIN INFRASTRUCTURE AND OTHER RESOURCES.—In carrying out subsection (b)(1), the Director shall leverage, to the greatest extent practicable, infrastructure and other resources provided under section 5.2 of the Executive Order dated October 30, 2023 (relating to safe, secure, and trustworthy development and use of artificial intelligence).

(d) ACCESS TO PROPRIETARY MODELS.—In carrying out this section, the Director shall establish such mechanisms as the Director considers appropriate, including potential contractual incentives, to ensure the provision of access to proprietary models by qualified independent third-party researchers if commercial model vendors have voluntarily provided models and associated resources for such testing.

(e) COUNTER-ARTIFICIAL INTELLIGENCE DEFINED.—In this section, the term ''counter-artificial intelligence'' means techniques or procedures to extract information about the behavior or characteristics of an artifi-

cial intelligence system, or to learn how to manipulate an artificial intelligence system, in order to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

SEC. 506. SENSE OF CONGRESS ENCOURAGING INTELLIGENCE COMMUNITY TO INCREASE PRIVATE SECTOR CAPITAL PARTNERSHIPS AND PARTNERSHIP WITH OFFICE OF STRATEGIC CAPITAL OF DEPARTMENT OF DEFENSE TO SECURE ENDURING TECHNOLOGICAL ADVANTAGES.

It is the sense of Congress that—

(1) acquisition leaders in the intelligence community should further explore the strategic use of private capital partnerships to secure enduring technological advantages for the intelligence community, including through the identification, development, and transfer of promising technologies to full-scale programs capable of meeting intelligence community requirements; and

(2) the intelligence community should undertake regular consultation with Federal partners, such as the Office of Strategic Capital of the Office of the Secretary of Defense, on best practices and lessons learned from their experiences integrating

these resources so as to accelerate attainment of national security objectives.

SEC. 507. INTELLIGENCE COMMUNITY TECHNOLOGY BRIDGE FUND.

(a) DEFINITIONS.—In this section:

(1) NONPROFIT ORGANIZATION.—The term ''nonprofit organization'' means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and that is exempt from tax under section 501(a) of such Code.

(2) WORK PROGRAM.—The term ''work program'' means any agreement between In-Q-Tel and a third-party company, where such third-party company furnishes or is furnishing a product or service for use by any of In-Q-Tel's government customers to address those customers' technology needs or requirements.

(b) ESTABLISHMENT OF FUND.—There is established in the Treasury of the United States a fund to be known as the ''Intelligence Community Technology Bridge Fund'' (in this subsection referred to as the ''Fund'') to assist in the transitioning of products or services from the research and development phase to the contracting and production phase.

(c) CONTENTS OF FUND.—The Fund shall consist of amounts appropriated to the Fund, and amounts in the Fund shall remain available until expended.

(d) AVAILABILITY AND USE OF FUND.—

(1) IN GENERAL.—Subject to paragraph (3), amounts in the Fund shall be available to the Director of National Intelligence to provide assistance to a business or nonprofit organization that is transitioning a product or service.

(2) TYPES OF ASSISTANCE.—Assistance provided under paragraph (1) may be distributed as funds in the form of a grant, a payment for a product or service, or a payment for equity.

(3) REQUIREMENTS FOR FUNDS.—Assistance may be provided under paragraph (1) to a business or nonprofit organization that is transitioning a product or service only if—

(A) the business or nonprofit organization—

(i) has participated or is participating in a work program; or

(ii) is engaged with an element of the intelligence community or Department of Defense for research and development; and

(B) the Director of National Intelligence or the head of an element of the intelligence community attests that the product or service will be utilized by an element of the intelligence community for a mission need, such as because it would be valuable in addressing a needed capability, fill or complement a technology gap, or increase the supplier base or price-competitiveness for the Federal Government.

(4) PRIORITY FOR SMALL BUSINESS CONCERNS AND NONTRADITIONAL DEFENSE CONTRACTORS.—In providing assistance under paragraph (1), the Director shall prioritize the provision of assistance to small business concerns (as defined under section 3(a) of the Small Business Act (15 U.S.C. 632(a))) and nontraditional defense contractors (as defined in section 3014 of title 10, United States Code).

(e) ADMINISTRATION OF FUND.—

(1) IN GENERAL.—The Fund shall be administered by the Director of National Intelligence.

(2) CONSULTATION.—In administering the Fund, the Director—

(A) shall consult with the heads of the elements of the intelligence community; and

(B) may consult with In-Q-Tel, the Defense Advanced Research Project Agency, the North Atlantic Treaty Organization Investment Fund, and the Defense Innovation Unit.

(f) ANNUAL REPORTS.—

(1) IN GENERAL.—Not later than September 30, 2025, and each fiscal year thereafter, the Director shall submit to the congressional intelligence committees a report on the Fund.

(2) CONTENTS.—Each report submitted pursuant to paragraph (1) shall include, for the period covered by the report, information about the following:

(A) How much was expended or obligated using amounts from the Fund.

(B) For what the amounts were expended or obligated.

(C) The effects of such expenditures and obligations.

(D) A summary of annual transition activities and outcomes of such activities for the intelligence community.

(3) FORM.—Each report submitted pursuant to paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(g) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—Subject to paragraph (2), there is authorized to be appropriated to the Fund $75,000,000 for fiscal year 2025 and for each fiscal year thereafter.

(2) LIMITATION.—The amount in the Fund shall not exceed $75,000,000 at any time.

SEC. 508. ENHANCEMENT OF AUTHORITY FOR INTELLIGENCE COMMUNITY PUBLIC-PRIVATE TALENT EXCHANGES.

(a) FOCUS AREAS.—Subsection (a) of section 5306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334) is amended—

(1) by striking ''Not later than'' and inserting the following:

''(1) IN GENERAL.—Not later than''; and

(2) by adding at the end the following:

''(2) FOCUS AREAS.—The Director shall ensure that the policies, processes, and procedures developed pursuant to paragraph (1) include a focus on rotations described in such paragraph with private-sector organizations in the following fields:

''(A) Finance.

''(B) Acquisition.

''(C) Biotechnology.

''(D) Computing.

''(E) Artificial intelligence.

''(F) Business process innovation and entrepreneurship.

''(G) Cybersecurity.

''(H) Materials and manufacturing.

''(I) Any other technology or research field the Director determines relevant to meet evolving national security threats in technology sectors.''.

(b) DURATION OF TEMPORARY DETAILS.—Subsection (e) of section 5306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334) is amended—

(1) in paragraph (1), by striking ''3 years'' and inserting ''5 years''; and

(2) in paragraph (2), by striking ''3 years'' and inserting ''5 years''.

(c) TREATMENT OF PRIVATE-SECTOR EMPLOYEES.—Subsection (g) of such section is amended—

(1) in paragraph (5), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(7) shall not be considered to have a conflict of interest with an element of the intelligence community solely because of being detailed to an element of the intelligence community under this section.''.

(d) HIRING AUTHORITY.—Such section is amended—

(1) by redesignating subsection (j) as subsection (k); and

(2) by inserting after subsection (i) the following:

''(j) HIRING AUTHORITY.—

''(1) IN GENERAL.—The Director may hire, under section 213.3102(r) of title 5, Code of Federal Regulations, or successor regulations, an individual who is an employee of a private-sector organization who is detailed to an element of the intelligence community under this section.

''(2) NO PERSONNEL BILLET REQUIRED.—Hiring an individual under paragraph (1) shall not require a personnel billet.''.

(e) ANNUAL REPORTS.—Not later than 1 year after the date of the enactment of this Act and annually there-

after for 2 more years, the Director of National Intelligence shall submit to the congressional intelligence committees an annual report on—

(1) the implementation of the policies, processes, and procedures developed pursuant to subsection (a) of such section 5306 (50 U.S.C. 3334) and the administration of such section;

(2) how the heads of the elements of the intelligence community are using or plan to use the authorities provided under such section; and

(3) recommendations for legislative or administrative action to increase use of the authorities provided under such section.

SEC. 509. ENHANCING INTELLIGENCE COMMUNITY ABILITY TO ACQUIRE EMERGING TECHNOLOGY THAT FULFILLS INTELLIGENCE COMMUNITY NEEDS.

(a) DEFINITION OF WORK PROGRAM.—The term ''work program'' means any agreement between In-Q-Tel and a third-party company, where such third-party company furnishes or is furnishing a property, product, or service for use by any of In-Q-Tel's government customers to address those customers' technology needs or requirements.

(b) IN GENERAL.—In addition to the exceptions listed under section 3304(a) of title 41, United States Code, and under section 3204(a) of title 10, United States Code, for the use of competitive procedures, the Director of National Intelligence or the head of an element of the intelligence community may use procedures other than competitive procedures to acquire a property, product, or service if—

(1) the source of the property, product, or service is a company that completed a work program in which the company furnished the property, product, or service; and

(2) the Director of National Intelligence or the head of an element of the intelligence community certifies that such property, product, or service has been shown to meet an identified need of the intelligence community.

(c) JUSTIFICATION FOR USE OF PROCEDURES OTHER THAN COMPETITIVE PROCEDURES.—

(1) IN GENERAL.—A property, product, or service may not be acquired by the Director or the head of an element of the intelligence community under subsection (b) using procedures other than competitive procedures unless the acquiring officer for the

acquisition justifies the use of such procedures in writing.

(2) CONTENTS.—A justification in writing described in paragraph (1) for an acquisition using procedures other than competitive procedures shall include the following:

(A) A description of the need of the element of the intelligence community that the property, product, or service satisfies.

(B) A certification that the anticipated costs will be fair and reasonable.

(C) A description of the market survey conducted or a statement of the reasons a market survey was not conducted.

(D) Such other matters as the Director or the head, as the case may be, determines appropriate.

SEC. 510. MANAGEMENT OF ARTIFICIAL INTELLIGENCE SECURITY RISKS.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE SAFETY INCIDENT.—The term ''artificial intelligence safety incident'' means an event that increases the risk that operation of an artificial intelligence system will—

(A) result in physical or psychological harm; or

(B) lead to a state in which human life, health, property, or the environment is endangered.

(2) ARTIFICIAL INTELLIGENCE SECURITY INCIDENT.—The term ''artificial intelligence security incident'' means an event that increases—

(A) the risk that operation of an artificial intelligence system occurs in a way that enables the extraction of information about the behavior or characteristics of an artificial intelligence system by a third party; or

(B) the ability of a third party to manipulate an artificial intelligence system to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

(3) ARTIFICIAL INTELLIGENCE SECURITY VULNERABILITY.—The term ''artificial intelligence security vulnerability'' means a weakness in an artificial intelligence system that could be exploited by a third party to, without authorization, subvert the confidentiality, integrity, or availability of an artificial

intelligence system, including through techniques such as—

(A) data poisoning;

(B) evasion attacks;

(C) privacy-based attacks; and

(D) abuse attacks.

(4) COUNTER-ARTIFICIAL INTELLIGENCE.—The term ''counter-artificial intelligence'' means techniques or procedures to extract information about the behavior or characteristics of an artificial intelligence system, or to learn how to manipulate an artificial intelligence system, so as to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

(b) VOLUNTARY TRACKING AND PROCESSING OF SECURITY AND SAFETY INCIDENTS AND RISKS ASSOCIATED WITH ARTIFICIAL INTELLIGENCE.—

(1) PROCESSES AND PROCEDURES FOR VULNERABILITY MANAGEMENT.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall—

(A) initiate a process to update processes and procedures associated with the National Vulnerability Database of the Institute to en-

sure that the database and associated vulnerability management processes incorporate artificial intelligence security vulnerabilities to the greatest extent practicable; and

(B) identify any characteristics of artificial intelligence security vulnerabilities that make utilization of the National Vulnerability Database inappropriate for their management and develop processes and procedures for vulnerability management of those vulnerabilities.

(2) VOLUNTARY TRACKING OF ARTIFICIAL INTELLIGENCE SECURITY AND ARTIFICIAL INTELLIGENCE SAFETY INCIDENTS.—

(A) VOLUNTARY DATABASE REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Director of the Institute, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(i) develop and establish a comprehensive database to publicly track artificial intelligence security and artificial intelligence safety incidents through voluntary input; and

(ii) in establishing the database under clause (i)—

(I) establish mechanisms by which private sector entities, public sector organizations, civil society groups, and academic researchers may voluntarily share information with the Institute on confirmed or suspected artificial intelligence security or artificial intelligence safety incidents, in a manner that preserves the confidentiality of any affected party;

(II) leverage, to the greatest extent possible, standardized disclosure and incident description formats;

(III) develop processes to associate reports pertaining to the same incident with a single incident identifier;

(IV) establish classification, information retrieval, and reporting mechanisms that sufficiently differentiate between artificial intelligence security incidents and artificial intelligence safety incidents; and

(V) create appropriate taxonomies to classify incidents based on relevant characteristics, impact, or other relevant criteria.

(B) IDENTIFICATION AND TREATMENT OF MATERIAL ARTIFICIAL INTELLIGENCE SECURITY OR ARTIFICIAL INTELLIGENCE SAFETY RISKS.—

(i) IN GENERAL.—Upon receipt of relevant information on an artificial intelligence security or artificial intelligence safety incident, the Director of the Institute shall determine whether the described incident presents a material artificial intelligence security or artificial intelligence safety risk sufficient for inclusion in the database developed and established under subparagraph (A).

(ii) PRIORITIES.—In evaluating a reported incident pursuant to subparagraph (A), the Director shall prioritize inclusion in the database cases in which a described incident—

(I) describes an artificial intelligence system used in critical infrastructure or safety-critical systems;

(II) would result in a high-severity or catastrophic impact to the people or economy of the United States; or

(III) includes an artificial intelligence system widely used in commercial or public sector contexts.

(C) REPORTS AND ANONYMITY.—The Director shall populate the database developed and established under subparagraph (A) with incidents based on public reports and information shared using the mechanism established pursuant to clause (ii)(I) of such subparagraph, ensuring that any incident description sufficiently anonymizes those affected, unless those who are affected have consented to their names being included in the database.

(c) UPDATING PROCESSES AND PROCEDURES RELATING TO COMMON VULNERABILITIES AND EXPOSURES PROGRAM AND EVALUATION OF CONSENSUS STANDARDS RELATING TO ARTIFICIAL INTELLIGENCE SECURITY VULNERABILITY REPORTING.—

(1) DEFINITIONS.—In this subsection:

(A) COMMON VULNERABILITIES AND EXPOSURES PROGRAM.—The term ''Common

Vulnerabilities and Exposures Program'' means the reference guide and classification system for publicly known information security vulnerabilities sponsored by the Cybersecurity and Infrastructure Security Agency.

(B) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(C) RELEVANT CONGRESSIONAL COMMITTEES.—The term ''relevant congressional committees'' means—

(i) the Committee on Homeland Security and Governmental Affairs of the Senate;

(ii) the Committee on Commerce, Science, and Transportation of the Senate;

(iii) the Select Committee on Intelligence of the Senate;

(iv) the Committee on the Judiciary of the Senate;

(v) the Committee on Oversight and Accountability of the House of Representatives;

(vi) the Committee on Energy and Commerce of the House of Representatives;

(vii) the Permanent Select Committee on Intelligence of the House of Representatives; and

(viii) the Committee on the Judiciary of the House of Representatives.

(2) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director shall—

(A) initiate a process to update processes and procedures associated with the Common Vulnerabilities and Exposures Program to ensure that the program and associated processes identify and enumerate artificial intelligence security vulnerabilities to the greatest extent practicable; and

(B) identify any characteristic of artificial intelligence security vulnerabilities that makes utilization of the Common Vulnerabilities and Exposures Program inappropriate for their management and develop processes and procedures for vulnerability identification and enu-

meration of those artificial intelligence security vulnerabilities.

(3) EVALUATION OF CONSENSUS STANDARDS.—

(A) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, the Director of the National Institute of Standards and Technology shall initiate a multi-stakeholder process to evaluate whether existing voluntary consensus standards for vulnerability reporting effectively accommodate artificial intelligence security vulnerabilities.

(B) REPORT.—

(i) SUBMISSION.—Not later than 180 days after the date on which the evaluation under subparagraph (A) is carried out, the Director shall submit a report to the relevant congressional committees on the sufficiency of existing vulnerability reporting processes and standards to accommodate artificial intelligence security vulnerabilities.

(ii) POST-REPORT ACTION.—If the Director concludes in the report submitted under clause (i) that existing processes do not sufficiently accommodate reporting of

artificial intelligence security vulnerabilities, the Director shall initiate a process, in consultation with the Director of the National Institute of Standards and Technology and the Director of the Office of Management and Budget, to update relevant vulnerability reporting processes, including the Department of Homeland Security Binding Operational Directive 20–01, or any subsequent directive.

(4) BEST PRACTICES.—Not later than 90 days after the date of enactment of this Act, the Director shall, in collaboration with the Director of the National Security Agency and the Director of the National Institute of Standards and Technology and leveraging efforts of the Information Communications Technology Supply Chain Risk Management Task Force to the greatest extent practicable, convene a multi-stakeholder process to encourage the development and adoption of best practices relating to addressing supply chain risks associated with training and maintaining artificial intelligence models, which shall ensure consideration of supply chain risks associated with—

(A) data collection, cleaning, and labeling, particularly the supply chain risks of reliance on remote workforce and foreign labor for such tasks;

(B) inadequate documentation of training data and test data storage, as well as limited provenance of training data;

(C) human feedback systems used to refine artificial intelligence systems, particularly the supply chain risks of reliance on remote workforce and foreign labor for such tasks;

(D) the use of large-scale, open-source datasets, particularly the supply chain risks to repositories that host such datasets for use by public and private sector developers in the United States; and

(E) the use of proprietary datasets containing sensitive or personally identifiable information.

SEC. 511. PROTECTION OF TECHNOLOGICAL MEASURES DESIGNED TO VERIFY AUTHENTICITY OR PROVENANCE OF MACHINE-MANIPULATED MEDIA.

(a) DEFINITIONS.—In this section:

(1) MACHINE-MANIPULATED MEDIA.—The term ''machine-manipulated media'' has the meaning

given such term in section 5724 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (Public Law 116–92; 50 U.S.C. 3024 note).

(2) STATE.—The term ''State'' means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

(b) PROHIBITIONS.—

(1) PROHIBITION ON CONCEALING SUBVERSION.—No person shall knowingly and with the intent or substantial likelihood of deceiving a third party, enable, facilitate, or conceal the subversion of a technological measure designed to verify the authenticity, modifications, or conveyance of machine-manipulated media, or characteristics of the provenance of the machine-manipulated media, by generating information about the authenticity of a piece of content that is knowingly false.

(2) PROHIBITION ON FRAUDULENT DISTRIBUTION.—No person shall knowingly and for financial benefit, enable, facilitate, or conceal the subversion of a technological measure described in paragraph (1) by distributing machine-manipulated media with

knowingly false information about the authenticity of a piece of machine-manipulated media.

(3) PROHIBITION ON PRODUCTS AND SERVICES FOR CIRCUMVENTION.—No person shall deliberately manufacture, import, or offer to the public a technology, product, service, device, component, or part thereof that—

(A) is primarily designed or produced and promoted for the purpose of circumventing, removing, or otherwise disabling a technological measure described in paragraph (1) with the intent or substantial likelihood of deceiving a third party about the authenticity of a piece of machine-manipulated media;

(B) has only limited commercially significant or expressive purpose or use other than to circumvent, remove, or otherwise disable a technological measure designed to verify the authenticity of machine-manipulated media and is promoted for such purposes; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing, removing, or otherwise disabling a technological measure described in paragraph (1) with an in-

tent to deceive a third party about the authenticity of a piece of machine-manipulated media.

(c) EXEMPTIONS.—

(1) IN GENERAL.—Nothing in subsection (b) shall inhibit the ability of any individual to access, read, or review a technological measure described in paragraph (1) of such subsection or to access, read, or review the provenance, modification, or conveyance information contained therein.

(2) EXEMPTION FOR NONPROFIT LIBRARIES, ARCHIVES, AND EDUCATIONAL INSTITUTIONS.—

(A) IN GENERAL.—Except as otherwise provided in this subsection, subsection (b) shall not apply to a nonprofit library, archives, or educational institution which generates, distributes, or otherwise handles machine-manipulated media.

(B) COMMERCIAL ADVANTAGE, FINANCIAL GAIN, OR TORTIOUS CONDUCT.—The exception in subparagraph (A) shall not apply to a nonprofit library, archive, or educational institution that willfully for the purpose of commercial advantage, financial gain, or in furtherance of tortious conduct violates a provision of subsection (b), except that a nonprofit library, ar-

chive, or educational institution that willfully for the purpose of commercial advantage, financial gain, or in furtherance of tortious conduct violates a provision of subsection (b) shall—

(i) for the first offense, be subject to the civil remedies under subsection (d); and

(ii) for repeated or subsequent offenses, in addition to the civil remedies under subsection (d), forfeit the exemption provided under subparagraph (A).

(C) CIRCUMVENTING TECHNOLOGIES.—This paragraph may not be used as a defense to a claim under paragraph (3) of subsection (b), nor may this subsection permit a nonprofit library, archive, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, that circumvents a technological measure described in paragraph (1) of such subsection.

(D) QUALIFICATIONS OF LIBRARIES AND ARCHIVES.—In order for a library or archive to qualify for the exemption under subparagraph

(A), the collections of that library or archive shall be—

(i) open to the public; or

(ii) available not only to researchers affiliated with the library or archive or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(3) REVERSE ENGINEERING.—

(A) DEFINITIONS.—In this paragraph:

(i) CIRCUMVENTION.—The term ''circumvention'' means to remove, deactivate, disable, or impair a technological measure designed to verify the authenticity of machine-manipulated media or characteristics of its provenance, modifications, or conveyance.

(ii) INTEROPERABILITY.—The term ''interoperability'' means the ability of—

(I) computer programs to exchange information; and

(II) such programs mutually to use the information which has been exchanged.

(B) IN GENERAL.—An authorized user of a technological measure described in subsection (b)(1) may circumvent such technological measure for the sole purpose of identifying and analyzing those elements of the technological measure that are necessary to achieve interoperability with that authorized user's own technological measures intended for similar purposes of verifying the authenticity of machine-manipulated media or characteristics of its provenance, modifications, or conveyance.

(C) LAW ENFORCEMENT, INTELLIGENCE, AND OTHER GOVERNMENT ACTIVITIES.—Subsection (b) does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State.

(d) ENFORCEMENT BY ATTORNEY GENERAL.—

(1) CIVIL ACTIONS.—The Attorney General may bring a civil action in an appropriate United

States district court against any person who violates subsection (b).

(2) POWERS OF THE COURT.—In an action brought under paragraph (1), the court—

(A) may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation, but in no event shall impose a prior restraint on free speech or the press protected under the First Amendment to the Constitution of the United States;

(B) at any time while an action is pending, may order the impounding, on such terms as it deems reasonable, of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation;

(C) may award damages under paragraph (3);

(D) in its discretion may allow the recovery of costs against any party other than the United States or an officer thereof; and

(E) may, as part of a final judgment or decree finding a violation, order the remedial modification or the destruction of any device or

product involved in the violation that is in the custody or control of the violator or has been impounded under subparagraph (B).

(3) AWARD OF DAMAGES.—

(A) IN GENERAL.—Except as otherwise provided in this section, a person committing a violation of subsection (b) is liable for statutory damages as provided in subparagraph (C).

(B) STATUTORY DAMAGES.—

(i) ELECTION OF AMOUNT BASED ON NUMBER OF ACTS OF CIRCUMVENTION.—At any time before final judgment is entered, the Attorney General may elect to recover an award of statutory damages for each violation of subsection (b) in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.

(ii) ELECTION OF AMOUNT; TOTAL AMOUNT.—At any time before final judgment is entered, the Attorney General may elect to recover an award of statutory damages for each violation of subsection (b) in

the sum of not less than $2,500 or more than $25,000.

(C) REPEATED VIOLATIONS.—In any case in which the Attorney General sustains the burden of proving, and the court finds, that a person has violated subsection (b) within 3 years after a final judgment was entered against the person for another such violation, the court may increase the award of damages up to triple the amount that would otherwise be awarded, as the court considers just.

(D) INNOCENT VIOLATIONS.—

(i) IN GENERAL.—The court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation.

(ii) NONPROFIT LIBRARY, ARCHIVE, EDUCATIONAL INSTITUTIONS, OR PUBLIC BROADCASTING ENTITIES.—In the case of a nonprofit library, archive, educational institution, or public broadcasting entity, the court shall remit damages in any case in

which the library, archive, educational institution, or public broadcasting entity sustains the burden of proving, and the court finds, that the library, archive, educational institution, or public broadcasting entity was not aware and had no reason to believe that its acts constituted a violation.

SEC. 512. SENSE OF CONGRESS ON HOSTILE FOREIGN CYBER ACTORS.

It is the sense of Congress that foreign ransomware organizations, and foreign affiliates associated with them, constitute hostile foreign cyber actors, that covered nations abet and benefit from the activities of these actors, and that such actors should be treated as hostile foreign cyber actors by the United States. Such actors include the following:

(1) DarkSide.

(2) Conti.

(3) REvil.

(4) BlackCat, also known as ''ALPHV''.

(5) LockBit.

(6) Rhysida, also known as ''Vice Society''.

(7) Royal.

(8) Phobos, also known as ''Eight'' and also known as ''Joanta''.

(9) C10p.

(10) Hackers associated with the SamSam ransomware campaigns.

(11) Play.

(12) BianLian.

(13) Killnet.

(14) Akira.

(15) Ragnar Locker, also known as ''Dark Angels''.

(16) Blacksuit.

(17) INC.

(18) Black Basta.

SEC. 513. DESIGNATION OF STATE SPONSORS OF RANSOMWARE AND REPORTING REQUIREMENTS.

(a) DESIGNATION OF STATE SPONSORS OF RANSOMWARE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Secretary of State, in consultation with the Director of National Intelligence, shall—

(A) designate as a state sponsor of ransomware any country the government of which the Secretary has determined has pro-

vided support for ransomware demand schemes (including by providing safe haven for individuals engaged in such schemes);

(B) submit to Congress a report listing the countries designated under subparagraph (A); and

(C) in making designations under subparagraph (A), take into consideration the report submitted to Congress under section 514(c)(1).

(2) SANCTIONS AND PENALTIES.—The President shall impose with respect to each state sponsor of ransomware designated under paragraph (1)(A) the sanctions and penalties imposed with respect to a state sponsor of terrorism.

(3) STATE SPONSOR OF TERRORISM DEFINED.—In this subsection, the term ''state sponsor of terrorism'' means a country the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism, for purposes of—

(A) section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(c)(1)(A)(i));

(B) section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371);

(C) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or

(D) any other provision of law.

(b) REPORTING REQUIREMENTS.—

(1) SANCTIONS RELATING TO RANSOMWARE REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Treasury shall submit a report to Congress that describes, for each of the 5 fiscal years immediately preceding the date of such report, the number and geographic locations of individuals, groups, and entities subject to sanctions imposed by the Office of Foreign Assets Control who were subsequently determined to have been involved in a ransomware demand scheme.

(2) COUNTRY OF ORIGIN REPORT.—The Secretary of State, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall—

(A) submit a report, with a classified annex, to the Committee on Foreign Relations of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Foreign Affairs of the House of Representatives, and the Permanent Select Committee on Intel-

ligence of the House of Representatives that identifies the country of origin of foreign-based ransomware attacks; and

(B) make the report described in subparagraph (A) (excluding the classified annex) available to the public.

(3) INVESTIGATIVE AUTHORITIES REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall issue a report that outlines the authorities available to the Federal Bureau of Investigation, the United States Secret Service, the Cybersecurity and Infrastructure Security Agency, Homeland Security Investigations, and the Office of Foreign Assets Control to respond to foreign-based ransomware attacks.

SEC. 514. DEEMING RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE A NATIONAL INTELLIGENCE PRIORITY.

(a) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term ''critical infrastructure'' has the meaning given such term in subsection (e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(b) RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE AS NATIONAL INTELLIGENCE PRIORITY.—

The Director of National Intelligence, pursuant to the provisions of the National Security Act of 1947 (50 U.S.C. 3001 et seq.), the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), section 1.3(b)(17) of Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), as in effect on the day before the date of the enactment of this Act, and National Security Presidential Directive–26 (February 24, 2003; relating to intelligence priorities), as in effect on the day before the date of the enactment of this Act, shall deem ransomware threats to critical infrastructure a national intelligence priority component to the National Intelligence Priorities Framework.

(c) REPORT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the implications of the ransomware threat to United States national security.

(2) CONTENTS.—The report submitted under paragraph (1) shall address the following:

(A) Identification of individuals, groups, and entities who pose the most significant threat, including attribution to individual ransomware attacks whenever possible.

(B) Locations from which individuals, groups, and entities conduct ransomware attacks.

(C) The infrastructure, tactics, and techniques ransomware actors commonly use.

(D) Any relationships between the individuals, groups, and entities that conduct ransomware attacks and their governments or countries of origin that could impede the ability to counter ransomware threats.

(E) Intelligence gaps that have impeded, or currently are impeding, the ability to counter ransomware threats.

(3) FORM.—The report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

TITLE VI—CLASSIFICATION REFORM

SEC. 601. GOVERNANCE OF CLASSIFICATION AND DECLASSIFICATION SYSTEM.

(a) DEFINITIONS.—In this section:

(1) CONTROLLED UNCLASSIFIED INFORMATION.—The term ''controlled unclassified information'' means information described as ''Controlled Unclassified Information'' or ''CUI'' in Executive Order 13556 (75 Fed. Reg. 68675; relating to controlled unclassified information), or any successor order.

(2) EXECUTIVE AGENT.—The term ''Executive Agent'' means the Executive Agent for Classification and Declassification designated under subsection (b)(1)(A).

(3) EXECUTIVE COMMITTEE.—The term ''Executive Committee'' means the Executive Committee on Classification and Declassification Programs and Technology established under subsection (b)(1)(C).

(b) ESTABLISHMENT OF CLASSIFICATION AND DECLASSIFICATION GOVERNANCE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President shall—

(A) designate a Federal official as Executive Agent for Classification and Declassification to identify and promote technological solutions to support efficient and effective systems for classification and declassification to be implemented on an interoperable and federated basis across the Federal Government;

(B) designate a Federal official—

(i) to establish policies and guidance relating to classification and declassification and controlled unclassified information across the Federal Government;

(ii) to conduct oversight of the implementation of such policies and guidance; and

(iii) who may, at the discretion of the President, also serve as Executive Agent; and

(C) establish an Executive Committee on Classification and Declassification Programs and Technology to provide direction, advice, and guidance to the Executive Agent.

(2) EXECUTIVE COMMITTEE.—

(A) COMPOSITION.—The Executive Committee shall be composed of the following or their designees:

(i) The Director of National Intelligence.

(ii) The Under Secretary of Defense for Intelligence and Security.

(iii) The Secretary of Energy.

(iv) The Secretary of State.

(v) The Director of the Office of Management and Budget.

(vi) The Archivist of the United States.

(vii) The Federal official designated under subsection (b)(1)(B) if such official is not also the Executive Agent.

(viii) Such other members as the Executive Agent considers appropriate.

(B) CHAIRPERSON.—The Executive Agent shall be the chairperson of the Executive Committee.

(c) REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the

President shall submit to Congress a report on the administration of this section.

(2) CONTENTS.—The report submitted pursuant to paragraph (1) shall include the following:

(A) Funding, personnel, expertise, and resources required for the Executive Agent and a description of how such funding, personnel, expertise, and resources will be provided.

(B) Authorities needed by the Executive Agent, a description of how such authorities will be granted, and a description of any additional statutory authorities required.

(C) Funding, personnel, expertise, and resources required by the Federal official designated under subsection (b)(1)(B) and a description of how such funding, personnel, expertise, and resources will be provided.

(D) Authorities needed by the Federal official designated under subsection (b)(1)(B), a description of how such authorities will be provided, and a description of any additional statutory authorities required.

(E) Funding and resources required by the Public Interest Declassification Board.

(d) PUBLIC REPORTING.—

(1) IN GENERAL.—The report required by subsection (c) shall be made available to the public to the greatest extent possible consistent with the protection of sources and methods.

(2) PUBLICATION IN FEDERAL REGISTER.—The President shall publish in the Federal Register the roles and responsibilities of the Federal officials designated under subsection (b), the Executive Committee, and any subordinate individuals or entities.

SEC. 602. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

(a) IN GENERAL.—Title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.) is amended by inserting after section 801 the following:

"SEC. 801A. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

"(a) IN GENERAL.—The President may, in accordance with this section, protect from unauthorized disclosure any information owned by, produced by or for, or under the control of the executive branch of the Federal Government when there is a demonstrable need to do so to protect the national security of the United States.

"(b) ESTABLISHMENT OF STANDARDS, CATEGORIES, AND PROCEDURES FOR CLASSIFICATION AND DECLASSIFICATION.—

"(1) GOVERNMENTWIDE PROCEDURES.—

"(A) CLASSIFICATION.—The President shall, to the extent necessary, establish categories of information that may be classified and procedures for classifying information under subsection (a).

"(B) DECLASSIFICATION.—At the same time the President establishes categories and procedures under subparagraph (A), the President shall establish procedures for declassifying information that was previously classified.

"(C) MINIMUM REQUIREMENTS.—The procedures established pursuant to subparagraphs (A) and (B) shall—

"(i) be the exclusive means for classifying information on or after the effective date established by subsection (c), except with respect to information classified pursuant to the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.);

"(ii) ensure that no information is classified unless there is a demonstrable need to do so to protect the national security and there is a reasonable basis to be-

lieve that means other than classification will not provide sufficient protection;

"(iii) ensure that no information may remain classified indefinitely;

"(iv) ensure that no information shall be classified, continue to be maintained as classified, or fail to be declassified in order—

"(I) to conceal violations of law, inefficiency, or administrative error;

"(II) to prevent embarrassment to a person, organization, or agency;

"(III) to restrain competition; or

"(IV) to prevent or delay the release of information that does not require protection in the interest of the national security;

"(v) ensure that basic scientific research information not clearly related to the national security shall not be classified;

"(vi) ensure that information may not be reclassified after being declassified and released to the public under proper authority unless personally approved by the President based on a determination that

such reclassification is required to prevent significant and demonstrable damage to the national security;

''(vii) establish standards and criteria for the classification of information;

''(viii) establish standards, criteria, and timelines for the declassification of information classified under this section;

''(ix) provide for the automatic declassification of classified records with permanent historical value not more than 50 years after the date of origin of such records, unless the head of each agency that classified information contained in such records makes a written determination to delay automatic declassification and such determination is reviewed not less frequently than every 10 years;

''(x) provide for the timely review of materials submitted for pre-publication;

''(xi) ensure that due regard is given for the public interest in disclosure of information;

''(xii) ensure that due regard is given for the interests of departments and agen-

cies in sharing information at the lowest possible level of classification;

"(D) SUBMITTAL TO CONGRESS.—The President shall submit to Congress the categories and procedures established under subsection (b)(1)(A) and the procedures established under subsection (b)(1)(B) at least 60 days prior to their effective date.

"(2) AGENCY STANDARDS AND PROCEDURES.—

"(A) IN GENERAL.—The head of each agency shall establish a single set of consolidated standards and procedures to permit such agency to classify and declassify information created by such agency in accordance with the categories and procedures established by the President under this section and otherwise to carry out this section.

"(B) SUBMITTAL TO CONGRESS.—Each agency head shall submit to Congress the standards and procedures established by such agency head under subparagraph (A).

"(c) EFFECTIVE DATE.—

"(1) IN GENERAL.—Subsections (a) and (b) shall take effect on the date that is 180 days after

the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025.

''(2) RELATION TO PRESIDENTIAL DIRECTIVES.—Presidential directives regarding classifying, safeguarding, and declassifying national security information, including Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), in effect on the day before the date of the enactment of this Act, as well as procedures issued pursuant to such Presidential directives, shall remain in effect until superseded by procedures issued pursuant to subsection (b).''.

(b) CONFORMING AMENDMENT.—Section 805(2) of such Act (50 U.S.C. 3164(2)) is amended by inserting ''section 801A,'' before ''Executive Order''.

(c) CLERICAL AMENDMENT.—The table of contents preceding section 2 of such Act is amended by inserting after the item relating to section 801 the following new item:

''Sec. 801A. Classification and declassification of information.''.

SEC. 603. MINIMUM STANDARDS FOR EXECUTIVE AGENCY INSIDER THREAT PROGRAMS.

(a) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' means any Executive agency as defined in section 105 of title 5, United States Code, any military department as

defined in section 102 of such title, and any other entity in the executive branch of the Federal Government that comes into the possession of classified information.

(2) CLASSIFIED INFORMATION.—The term ''classified information'' means information that has been determined to require protection from unauthorized disclosure pursuant to Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or predecessor or successor order, to protect the national security of the United States.

(b) ESTABLISHMENT OF INSIDER THREAT PROGRAMS.—Each head of an agency with access to classified information shall establish an insider threat program to protect classified information from unauthorized disclosure.

(c) MINIMUM STANDARDS.—In carrying out an insider threat program established by the head of an agency pursuant to subsection (b), the head of the agency shall—

(1) designate a senior official of the agency who shall be responsible for management of the program;

(2) monitor user activity on all classified networks to detect activity indicative of insider threat behavior;

(3) build and maintain an insider threat analytic and response capability to review, assess, and respond to information obtained pursuant to paragraph (2); and

(4) provide insider threat awareness training to all cleared employees within 30 days of entry-on-duty or granting of access to classified information and annually thereafter.

(d) ANNUAL REPORTS.—Not less frequently than once each year, the Director of National Intelligence shall, serving as the Security Executive Agent under section 803 of the National Security Act of 1947 (50 U.S.C. 3162a), submit to Congress an annual report on the compliance of agencies with respect to the requirements of this section.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

SEC. 701. SECURITY CLEARANCES HELD BY CERTAIN FORMER EMPLOYEES OF INTELLIGENCE COMMUNITY.

(a) ISSUANCE OF GUIDELINES AND INSTRUCTIONS REQUIRED.—Section 803(c) of the National Security Act of 1947 (50 U.S.C. 3162a(c)) is amended—

(1) in paragraph (3), by striking ''; and'' and inserting a semicolon;

(2) in paragraph (4), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(5) issue guidelines and instructions to the heads of Federal agencies to ensure that any individual who was appointed by the President to a position in an element of the intelligence community but is no longer employed by the Federal Government shall maintain a security clearance only in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information), or successor order.''.

(b) SUBMITTAL OF GUIDELINES AND INSTRUCTIONS TO CONGRESS REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in the Director's capacity as the Security Executive Agent pursuant to subsection (a) of section 803 of the National Security Act of 1947 (50 U.S.C. 3162a), submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) the guidelines and instructions required by subsection

(c)(5) of such Act, as added by subsection (a) of this section.

(c) ANNUAL REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once each year thereafter, the Director of National Intelligence shall, in the Director's capacity as the Security Executive Agent pursuant to section 803(a) of the National Security Act of 1947 (50 U.S.C. 3162a(a)), submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) an annual report on the eligibility status of former senior employees of the intelligence community to access classified information.

(2) CONTENTS.—Each report submitted pursuant to paragraph (1) shall include, for the period covered by the report, the following:

(A) A list of individuals who were appointed by the President to a position in an element of the intelligence community who currently hold security clearances.

(B) The number of such former employees who still hold security clearances.

(C) For each former employee described in subparagraph (B)—

(i) the position in the intelligence community held by the former employee;

(ii) the years of service in such position; and

(iii) the individual's current employment position and employer.

(D) The Federal entity authorizing and adjudicating the former employees' need to know classified information.

SEC. 702. POLICY FOR AUTHORIZING INTELLIGENCE COMMUNITY PROGRAM OF CONTRACTOR-OWNED AND CONTRACTOR-OPERATED SENSITIVE COMPARTMENTED INFORMATION FACILITIES.

(a) POLICY.—The Director of National Intelligence shall establish a standardized policy for the intelligence community that authorizes a program of contractor-owned and contractor-operated sensitive compartmented information facilities as a service to the national security and intelligence enterprises.

(b) REQUIREMENTS.—The policy established pursuant to subsection (a) shall—

(1) authorize the head of an element of the intelligence community to approve and accredit contractor-owned and contractor-operated sensitive compartmented information facilities; and

(2) designate an element of the intelligence community as a service of common concern (as defined in Intelligence Community Directive 122, or successor directive) to serve as an accrediting authority on behalf of other elements of the intelligence community for contractor-owned and contractor-operated sensitive compartmented information facilities.

(c) COST CONSIDERATIONS.—In establishing the policy required by subsection (a), the Director shall consider existing demonstrated models where a contractor acquires, outfits, and manages a facility pursuant to an agreement with the Federal Government such that no funding from the Federal Government is required to carry out the agreement.

(d) BRIEFING REQUIRED.—Not later than 1 year after the date on which the Director establishes the policy pursuant to subsection (a), the Director shall brief the congressional intelligence committees on—

(1) additional opportunities to leverage contractor-provided secure facility space; and

(2) recommendations to address barriers, including resources or authorities needed.

SEC. 703. ENABLING INTELLIGENCE COMMUNITY INTEGRATION.

(a) IN GENERAL.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended by inserting after section 113B the following new section:

"SEC. 113C. ENABLING INTELLIGENCE COMMUNITY INTEGRATION.

''(a) PROVISION OF GOODS OR SERVICES.—Subject to and in accordance with any guidance and requirements developed by the Director of National Intelligence, the head of an element of the intelligence community may provide goods or services to another element of the intelligence community without reimbursement or transfer of funds for hoteling initiatives for intelligence community employees and affiliates defined in any such guidance and requirements issued by the Director of National Intelligence.

''(b) APPROVAL.—Prior to the provision of goods or services pursuant to subsection (a), the head of the element of the intelligence community providing such goods or services and the head of the element of the intelligence community receiving such goods or services shall approve such provision.''.

(b) CLERICAL AMENDMENT.—The table of contents of the National Security Act of 1947 is amended by inserting after the item relating to section 113B the following:

"Sec. 113C. Enabling intelligence community integration.".

SEC. 704. APPOINTMENT OF SPOUSES OF CERTAIN FEDERAL EMPLOYEES.

(a) IN GENERAL.—Section 3330d of title 5, United States Code, is amended—

(1) in the section heading, by striking "**military and Department of Defense civilian spouses**" and inserting "**military and Department of Defense, Department of State, and intelligence community spouses**";

(2) in subsection (a)—

(A) by redesignating the second paragraph (4) (relating to a spouse of an employee of the Department of Defense) as paragraph (7);

(B) by striking paragraph (5);

(C) by redesignating paragraph (4) (relating to the spouse of a disabled or deceased member of the Armed Forces) as paragraph (6);

(D) by striking paragraph (3) and inserting the following:

"(3) The term 'covered spouse' means an individual who is married to an individual who—

"(A)(i) is an employee of the Department of State or an element of the intelligence community; or

"(ii) is a member of the Armed Forces who is assigned to an element of the intelligence community; and

"(B) is transferred in the interest of the Government from one official station within the applicable agency to another within the agency (that is outside of normal commuting distance) for permanent duty.

"(4) The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

"(5) The term 'remote work' refers to a work flexibility arrangement under which an employee—

"(A) is not expected to physically report to the location from which the employee would otherwise work, considering the position of the employee; and

"(B) performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite—

"(i) other than the location from which the employee would otherwise work;

"(ii) that may be inside or outside the local commuting area of the location from which the employee would otherwise work; and

"(iii) that is typically the residence of the employee."; and

(E) by adding at the end the following:

"(8) The term 'telework' has the meaning given the term in section 6501."; and

(3) in subsection (b)—

(A) in paragraph (2), by striking "or" at the end;

(B) in the first paragraph (3) (relating to a spouse of a member of the Armed Forces on active duty), by striking the period at the end and inserting a semicolon;

(C) by redesignating the second paragraph (3) (relating to a spouse of an employee of the Department of Defense) as paragraph (4);

(D) in paragraph (4), as so redesignated—

(i) by inserting ", including to a position in which the spouse will engage in remote work" after "Department of Defense"; and

(ii) by striking the period at the end and inserting ''; or''; and

(E) by adding at the end the following:

''(5) a covered spouse to a position in which the covered spouse will engage in remote work.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subchapter I of chapter 33 of title 5, United States Code, is amended by striking the item relating to section 3330d and inserting the following:

''3330d. Appointment of military and Department of Defense, Department of State, and intelligence community civilian spouses.''.

SEC. 705. PLAN FOR STAFFING THE INTELLIGENCE COLLECTION POSITIONS OF THE CENTRAL INTELLIGENCE AGENCY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall submit to the congressional intelligence committees a plan for ensuring that the Directorate of Operations of the Agency has staffed every civilian full-time equivalent position authorized for that Directorate under the Intelligence Authorization Act for Fiscal Year 2024 (division G of Public Law 118–31).

(b) ELEMENTS.—The plan required by subsection (a) shall include the following:

(1) Specific benchmarks and timelines for accomplishing the goal described in such subsection by September 30, 2025.

(2) An assessment of the appropriate balance of staffing between the Directorate of Operations and the Directorate of Analysis consistent with the responsibilities of the Director of the Central Intelligence Agency under section 104A(d) of the National Security Act of 1947 (50 U.S.C. 3036(d)).

SEC. 706. INTELLIGENCE COMMUNITY WORKPLACE PROTECTIONS.

(a) EMPLOYMENT STATUS.—

(1) CONVERSION OF POSITIONS BY DIRECTOR OF NATIONAL INTELLIGENCE TO EXCEPTED SERVICE.—Section 102A(v) of the National Security Act of 1947 (50 U.S.C. 3024(v)) is amended—

(A) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively;

(B) by inserting after paragraph (1) the following:

''(2) The Director shall promptly notify the congressional intelligence committees of any action taken pursuant to paragraph (1).''; and

(C) in paragraph (3), as redesignated by subparagraph (A), by striking ''occupying a position on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2012''.

(2) CONVERSION OF DEFENSE INTELLIGENCE POSITIONS TO EXCEPTED SERVICE.—Section 1601(a) of title 10, United States Code, is amended—

(A) by redesignating subsection (b) as subsection (d); and

(B) by inserting after subsection (a) the following:

''(b) CONGRESSIONAL NOTIFICATION.—The Secretary shall promptly notify the congressional defense committees and the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) of any action taken pursuant to subsection (a).

''(c) RETENTION OF ACCRUED RIGHTS UPON CONVERSION.—An incumbent whose position is selected to be converted, without regard to the wishes of the incumbent, to the excepted service under subsection (a) shall remain in the competitive service for the purposes of status and any accrued adverse action protections while the individual

occupies that position or any other position to which the employee is moved involuntarily. Once such individual no longer occupies the converted position, the position may be treated as a regularly excepted service position.''.

(3) CONVERSION WITHIN THE EXCEPTED SERVICE.—An intelligence community incumbent employee whose position is selected to be converted from one excepted service schedule to another schedule within the excepted service without regard to the wishes of the incumbent shall remain in the current schedule for the purpose of status and any accrued adverse action protections while the individual occupies that position or any other position to which the employee is moved without regard to the wishes of the employee.

(b) CONGRESSIONAL NOTIFICATION OF GUIDELINES.—

(1) SUBMITTAL TO CONGRESS.—Not later than 30 days after the date of the enactment of this Act, each head of an element of the intelligence community shall submit to the congressional intelligence committees the guidelines and regulations of the element relating to employment status and protections relating to that status.

(2) NOTICE OF CHANGES.—In any case in which a guideline or regulation of an element of the intelligence community submitted pursuant to paragraph (1) is modified or replaced, the head of the element shall promptly notify the congressional intelligence committees of the change and submit the new or modified guideline or regulation.

(c) TERMINATION AUTHORITIES OF THE DIRECTOR OF THE CIA.—

(1) PROCESS AND NOTIFICATION.—Section 104A(e) of the National Security Act of 1947 (50 U.S.C. 3036(e)) is amended—

(A) by redesignating paragraph (2) as paragraph (3); and

(B) by inserting after paragraph (1) the following:

''(2)(A) Subject to subparagraph (B), the Director shall not take an action under paragraph (1) to terminate the employment of an officer or employee, except in accordance with guidelines and regulations submitted to the congressional intelligence committees.

''(B) The Director may take an action under paragraph (1) without or in contravention of the guidelines and regulations specified in subparagraph (A) of this paragraph if the Director determines that complying with

such guidelines and regulations poses a threat to the national security of the United States. If the Director makes such a determination, the Director shall provide prompt notification to the congressional intelligence committees that includes—

''(i) an explanation for the basis for the termination and the factual support for such determination; and

''(ii) an explanation for the determination that the process described in subparagraph (A) poses a threat to the national security of the United States.''.

(d) IMPROVEMENT OF CONGRESSIONAL NOTICE REQUIREMENT RELATING TO TERMINATION OF DEFENSE INTELLIGENCE EMPLOYEES.—Section 1609(c) of title 10, United States Code, is amended by adding at the end the following: ''Such notification shall include the following:

''(1) An explanation for the determination that the termination was in the interests of the United States.

''(2) An explanation for the determination that the procedures prescribed in other provisions of law that authorize the termination of the employment of such employee cannot be invoked in a manner con-

sistent with the national security of the United States.''.

(e) CONGRESSIONAL NOTIFICATION OF OTHER SUSPENSION AND REMOVAL AUTHORITIES.—Section 7532 of title 5, United States Code, is amended by adding at the end the following:

''(d)(1) The head of an element of the intelligence community who takes an action under this section shall promptly notify the congressional intelligence committees of such action.

''(2) Each notification under paragraph (1) regarding an action shall include the following:

''(A) An explanation for the determination that the action is necessary or advisable in the interests of national security.

''(B) If the head of an element of the intelligence community determines, pursuant to subsection (a), that the interests of national security do not permit notification to the employee of the reasons for the action under that subsection, an explanation for such determination.

''(3) In this subsection, the terms 'congressional intelligence committees' and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).''.

(f) SAVINGS CLAUSE.—Nothing in this section shall be construed to diminish the rights conferred by chapter 75 of title 5, United States Code, or other applicable agency adverse action or disciplinary procedures.

SEC. 707. SENSE OF CONGRESS ON GOVERNMENT PERSONNEL SUPPORT FOR FOREIGN TERRORIST ORGANIZATIONS.

It is the sense of Congress that for the purposes of adjudicating the eligibility of an individual for access to classified information, renewal of a prior determination of eligibility for such access, or continuous vetting of an individual for eligibility for such access, including on form SF–86 or any successor form, each of the following should be considered an action advocating for an act of terrorism:

(1) Espousing the actions of an organization designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(2) Advocating for continued attacks by an organization described in paragraph (1).

(3) Soliciting funds for an organization described in paragraph (1).

TITLE VIII—WHISTLEBLOWERS

SEC. 801. IMPROVEMENTS REGARDING URGENT CONCERNS SUBMITTED TO INSPECTORS GENERAL OF THE INTELLIGENCE COMMUNITY.

(a) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—Section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)) is amended—

(1) in subparagraph (A)—

(A) by inserting ''(i)'' before ''An employee of'';

(B) by inserting ''in writing'' before ''to the Inspector General''; and

(C) by adding at the end the following:

''(ii) The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this subparagraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.'';

(2) by striking subparagraph (B) and inserting the following:

''(B)(i)(I) Not later than the end of the period specified in subclause (II), the Inspector General shall determine whether the written complaint or information sub-

mitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

''(II) The period specified in this subclause is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subparagraph (A) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subparagraph.

''(ii) The Inspector General may transmit a complaint or information submitted under subparagraph (A) directly to the congressional intelligence committees—

''(I) without transmittal to the Director if the Inspector General determines that transmittal to the Director could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(II) following transmittal to the Director if the Director does not transmit the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C).'';

(3) in subparagraph (D)—

(A) in clause (i), by striking ''or does not transmit the complaint or information to the Director in accurate form under subparagraph (B),'' and inserting ''does not transmit the complaint or information to the Director in accurate form under subparagraph (B)(i)(I), or makes a determination pursuant to subparagraph (B)(ii)(I) but does not transmit the complaint or information to the congressional intelligence committees within 21 calendar days of receipt,''; and

(B) by striking clause (ii) and inserting the following:

''(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if—

''(I) the employee, before making such a contact—

''(aa) transmits to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

''(bb) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices; or

''(II) the Inspector General—

''(aa) determines that—

''(AA) a transmittal under subclause (I) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(BB) the Director has failed to provide adequate direction pursuant to item (bb) of subclause (I) within 7 calendar days of a transmittal under such subclause; and

''(bb) provides the employee direction on how to contact the congressional intelligence committees in accordance with appropriate security practices.''; and

(4) by adding at the end the following:

''(J) In this paragraph, the term 'employee', with respect to an employee of an element of the intelligence com-

munity, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who may submit a complaint or information to the Inspector General under subparagraph (A), means—

''(i) a current employee at the time of such submission; or

''(ii) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.''.

(b) INSPECTOR GENERAL OF THE CENTRAL INTELLIGENCE AGENCY.—Section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) is amended—

(1) in subparagraph (A)—

(A) by inserting (i) before ''An employee'';

(B) by inserting ''in writing'' before ''to the Inspector General''; and

(C) by adding at the end the following:

''(ii) The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this subparagraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or informa-

tion and treat such written record as a written submission.'';

(2) in subparagraph (B)—

(A) by striking clause (i) and inserting the following:

''(i)(I) Not later than the end of the period specified in subclause (II), the Inspector General shall determine whether the written complaint or information submitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

''(II) The period specified in this subclause is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subparagraph (A) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subparagraph.''; and

(B) by adding at the end the following:

''(iii) The Inspector General may transmit a complaint or information submitted under subparagraph (A) directly to the congressional intelligence committees—

''(I) without transmittal to the Director if the Inspector General determines that transmittal to the

Director could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information;

''(II) following transmittal to the Director if the Director does not transmit the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C) and has not made a determination regarding a conflict of interest pursuant to clause (ii); or

''(III) following transmittal to the Director and a determination by the Director that a conflict of interest exists pursuant to clause (ii) if the Inspector General determines that—

''(aa) transmittal to the Director of National Intelligence could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(bb) the Director of National Intelligence has not transmitted the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C).'';

(3) in subparagraph (D)—

(A) in clause (i), by striking ''or does not transmit the complaint or information to the Director in accurate form under subparagraph (B),'' and inserting ''does not transmit the complaint or information to the Director in accurate form under subparagraph (B)(i)(I), or makes a determination pursuant to subparagraph (B)(iii)(I) but does not transmit the complaint or information to the congressional intelligence committees within 21 calendar days of receipt,''; and

(B) by striking clause (ii) and inserting the following:

''(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if—

''(I) the employee, before making such a contact—

''(aa) transmits to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

''(bb) obtains and follows from the Director, through the Inspector General, direction on

how to contact the congressional intelligence committees in accordance with appropriate security practices; or

''(II) the Inspector General—

''(aa) determines that—

''(AA) the transmittal under subclause (I) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

''(BB) the Director has failed to provide adequate direction pursuant to item (bb) of subclause (I) within 7 calendar days of a transmittal under such subclause; and

''(bb) provides the employee direction on how to contact the congressional intelligence committees in accordance with appropriate security practices.''; and

(4) by adding at the end the following:

''(I) In this paragraph, the term 'employee', with respect to an employee of the Agency, or of a contractor to the Agency, who may submit a complaint or information to the Inspector General under subparagraph (A), means—

''(i) a current employee at the time of such submission; or

''(ii) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.''.

(c) OTHER INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.—Section 416 of title 5, United States Code, is amended—

(1) in subsection (a)—

(A) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively; and

(B) by inserting before paragraph (2), as redesignated by paragraph (1), the following:

''(1) EMPLOYEE.—The term 'employee', with respect to an employee of an element of the Federal Government covered by subsection (b), or of a contractor to such an element, who may submit a complaint or information to an Inspector General under such subsection, means—

''(A) a current employee at the time of such submission; or

''(B) a former employee at the time of such submission, if such complaint or informa-

tion arises from and relates to the period of employment as such an employee.'';

(2) in subsection (b)—

(A) in paragraph (1)—

(i) in the paragraph heading, by inserting ''; SUPPORT FOR WRITTEN SUBMISSION''; after ''MADE'';

(ii) by inserting ''in writing'' after ''may report the complaint or information'' each place it appears; and

(iii) in subparagraph (B), by inserting ''in writing'' after ''such complaint or information''; and

(B) by adding at the end the following:

''(E) SUPPORT FOR WRITTEN SUBMISSION.—The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this paragraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.'';

(3) in subsection (c)—

(A) by striking paragraph (1) and inserting the following:

''(1) CREDIBILITY.—

''(A) DETERMINATION.—Not later than the end of the period specified in subparagraph (B), the Inspector General shall determine whether the written complaint or information submitted under subsection (b) appears credible. Upon making such a determination, the Inspector General shall transmit to the head of the establishment notice of that determination, together with the complaint or information.

''(B) PERIOD SPECIFIED.—The period specified in this subparagraph is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subsection (b) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subsection.''; and

(B) by adding at the end the following:

''(3) TRANSMITTAL DIRECTLY TO INTELLIGENCE COMMITTEES.—The Inspector General may

transmit the complaint or information directly to the intelligence committees—

''(A) without transmittal to the head of the establishment if the Inspector General determines that transmittal to the head of the establishment could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information;

''(B) following transmittal to the head of the establishment if the head of the establishment does not transmit the complaint or information to the intelligence committees within the time period specified in subsection (d) and has not made a determination regarding a conflict of interest pursuant to paragraph (2); or

''(C) following transmittal to the head of the establishment and a determination by the head of the establishment that a conflict of interest exists pursuant to paragraph (2) if the Inspector General determines that—

''(i) transmittal to the Director of National Intelligence or the Secretary of Defense could compromise the anonymity of the employee or result in the complaint or

information being transmitted to a subject of the complaint or information; or

''(ii) the Director of National Intelligence or the Secretary of Defense has not transmitted the complaint or information to the intelligence committees within the time period specified in subsection (d).'';

(4) in subsection (e)(1), by striking ''or does not transmit the complaint or information to the head of the establishment in accurate form under subsection (c),'' and inserting ''does not transmit the complaint or information to the head of the establishment in accurate form under subsection (c)(1)(A), or makes a determination pursuant to subsection (c)(3)(A) but does not transmit the complaint or information to the intelligence committees within 21 calendar days of receipt,''; and

(5) in subsection (e), by striking paragraph (2) and inserting the following:

''(2) LIMITATION.—An employee may contact the intelligence committees directly as described in paragraph (1) only if—

''(A) the employee, before making such a contact—

"(i) transmits to the head of the establishment, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

"(ii) obtains and follows from the head of the establishment, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices; or

"(B) the Inspector General—

"(i) determines that the transmittal under subparagraph (A) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(ii) determines that the head of the establishment has failed to provide adequate direction pursuant to clause (ii) of subparagraph (A) within 7 calendar days of a transmittal under such subparagraph; and

''(iii) provides the employee direction on how to contact the intelligence committees in accordance with appropriate security practices.''.

SEC. 802. PROHIBITION AGAINST DISCLOSURE OF WHISTLEBLOWER IDENTITY AS ACT OF REPRISAL.

(a) IN GENERAL.—Section 1104(a) of the National Security Act of 1947 (50 U.S.C. 3234(a)) is amended—

(1) in paragraph (3)—

(A) in subparagraph (I), by striking ''; or'' and inserting a semicolon;

(B) by redesignating subparagraph (J) as subparagraph (K); and

(C) by inserting after subparagraph (I) the following:

''(J) an unauthorized whistleblower identity disclosure;''; and

(2) by adding at the end the following:

''(5) UNAUTHORIZED WHISTLEBLOWER IDENTITY DISCLOSURE.—The term 'unauthorized whistleblower identity disclosure' means, with respect to an employee or a contractor employee described in paragraph (3), a knowing and willful disclosure revealing the identity or other personally identifiable information of the employee or contractor employee

so as to identify the employee or contractor employee as an employee or contractor employee who has made a lawful disclosure described in subsection (b) or (c), but does not include such a knowing and willful disclosure that meets any of the following criteria:

''(A) Such disclosure was made with the express consent of the employee or contractor employee.

''(B) Such disclosure was made during the course of reporting or remedying the subject of the lawful disclosure of the whistleblower through management, legal, or oversight processes, including such processes relating to human resources, equal opportunity, security, or an Inspector General.

''(C) An Inspector General with oversight responsibility for the relevant covered intelligence community element determines that such disclosure—

''(i) was unavoidable under section 103H of this Act (50 U.S.C. 3033), section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517), section 407

of title 5, United States Code, or section 420(b)(2)(B) of such title;

''(ii) was made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; or

''(iii) was required by statute or an order from a court of competent jurisdiction.''.

(b) PRIVATE RIGHT OF ACTION FOR UNLAWFUL DISCLOSURE OF WHISTLEBLOWER IDENTITY.—Subsection (f) of such section is amended to read as follows:

''(f) ENFORCEMENT.—

''(1) IN GENERAL.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section.

''(2) HARMONIZATION WITH OTHER ENFORCEMENT.—To the fullest extent possible, the President shall provide for enforcement of this section in a manner that is consistent with the enforcement of section 2302(b)(8) of title 5, United States Code, especially with respect to policies and procedures used to adjudicate alleged violations of such section.

''(3) PRIVATE RIGHT OF ACTION FOR DISCLOSURES OF WHISTLEBLOWER IDENTITY IN VIOLATION

OF PROHIBITION AGAINST REPRISALS.—Subject to paragraph (4), in a case in which an employee of an agency takes a personnel action described in subsection (a)(3)(J) against an employee of a covered intelligence community element as a reprisal in violation of subsection (b) or in a case in which an employee or contractor employee takes a personnel action described in subsection (a)(3)(J) against another contractor employee as a reprisal in violation of subsection (c), the employee or contractor employee against whom the personnel action was taken may, consistent with section 1221 of title 5, United States Code, bring a private action for all appropriate remedies, including injunctive relief and compensatory and punitive damages, in an amount not to exceed $250,000, against the agency of the employee or contracting agency of the contractor employee who took the personnel action, in a Federal district court of competent jurisdiction.

''(4) REQUIREMENTS.—

''(A) REVIEW BY INSPECTOR GENERAL AND BY EXTERNAL REVIEW PANEL.—Before the employee or contractor employee may bring a private action under paragraph (3), the em-

ployee or contractor employee shall exhaust administrative remedies by—

"(i) first, obtaining a disposition of their claim by requesting review by the appropriate inspector general; and

"(ii) second, if the review under clause (i) does not substantiate reprisal, by submitting to the Inspector General of the Intelligence Community a request for a review of the claim by an external review panel under section 1106.

"(B) PERIOD TO BRING ACTION.—The employee or contractor employee may bring a private right of action under paragraph (3) during the 180-day period beginning on the date on which the employee or contractor employee is notified of the final disposition of their claim under section 1106.".

SEC. 803. PROTECTION FOR INDIVIDUALS MAKING AUTHORIZED DISCLOSURES TO INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.

(a) INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY.—Section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 3033(g)(3)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(2) by adding at the end the following new subparagraph:

''(B) An individual may disclose classified information to the Inspector General in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or section 803, chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.), or any applicable provision of law. Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

''(i) any otherwise applicable nondisclosure agreement;

''(ii) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information) or

chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

''(iii) section 798 of title 18, United States Code, or any other provision of law relating to the unauthorized disclosure of national security information.''; and

(3) in the paragraph enumerator, by striking ''(3) '' and inserting ''(3)(A)''.

(b) INSPECTOR GENERAL OF THE CENTRAL INTELLIGENCE AGENCY.—Section 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(e)(3)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(2) by adding at the end the following new subparagraph:

''(B) An individual may disclose classified information to the Inspector General in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or 803 of the National Security Act of 1947 (50 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure of classified

information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

"(i) any otherwise applicable nondisclosure agreement;

"(ii) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

"(iii) section 798 of title 18, United States Code, or any other provision of law relating to the unauthorized disclosure of national security information."; and

(3) in the paragraph enumerator, by striking "(3) " and inserting "(3)(A)".

(c) OTHER INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.—Section 416 of title 5, United States Code, is amended by adding at the end the following new subsection:

"(i) PROTECTION FOR INDIVIDUALS MAKING AUTHORIZED DISCLOSURES.—An individual may disclose

classified information to an Inspector General of an element of the intelligence community in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or 803 of the National Security Act of 1947 (50 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

''(1) any otherwise applicable nondisclosure agreement;

''(2) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

''(3) section 798 of title 18, or any other provision of law relating to the unauthorized disclosure of national security information.''.

SEC. 804. CLARIFICATION OF AUTHORITY OF CERTAIN INSPECTORS GENERAL TO RECEIVE PROTECTED DISCLOSURES.

Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (b)(1), by inserting ''or covered intelligence community element'' after ''the appropriate inspector general of the employing agency''; and

(2) in subsection (c)(1)(A), by inserting ''or covered intelligence community element'' after ''the appropriate inspector general of the employing or contracting agency''.

SEC. 805. WHISTLEBLOWER PROTECTIONS RELATING TO PSYCHIATRIC TESTING OR EXAMINATION.

(a) PROHIBITED PERSONNEL PRACTICES.—Section 1104(a)(3) of the National Security Act of 1947 (50 U.S.C. 3234(a)(3)) is amended—

(1) in subparagraph (I), by striking ''; or'' and inserting a semicolon;

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following new subparagraph:

''(J) a decision to order psychiatric testing or examination; or''.

(b) APPLICATION.—The amendments made by this section shall apply with respect to matters arising under section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) on or after the date of the enactment of this Act.

SEC. 806. ESTABLISHING PROCESS PARITY FOR ADVERSE SECURITY CLEARANCE AND ACCESS DETERMINATIONS.

Subparagraph (C) of section 3001(j)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(4)) is amended to read as follows:

"(C) CONTRIBUTING FACTOR.—

"(i) IN GENERAL.—Subject to clause (iii), in determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if the individual has demonstrated that a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual.

"(ii) CIRCUMSTANTIAL EVIDENCE.—An individual under clause (i) may demonstrate that the disclosure was a contrib-

uting factor in the adverse security clearance or access determination taken against the individual through circumstantial evidence, such as evidence that—

''(I) the official making the determination knew of the disclosure; and

''(II) the determination occurred within a period such that a reasonable person could conclude that the disclosure was a contributing factor in the determination.

''(iii) DEFENSE.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall not find that paragraph (1) was violated if, after a finding that a disclosure was a contributing factor, the agency demonstrates by clear and convincing evidence that it would have made the same security clearance or access determination in the absence of such disclosure.''.

SEC. 807. ELIMINATION OF CAP ON COMPENSATORY DAMAGES FOR RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.

Section 3001(j)(4)(B) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(4)(B)) is amended, in the second sentence, by striking ''not to exceed $300,000''.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

SEC. 901. ADDITIONAL DISCRETION FOR DIRECTOR OF CENTRAL INTELLIGENCE AGENCY IN PAYING COSTS OF TREATING QUALIFYING INJURIES AND MAKING PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.

(a) ADDITIONAL AUTHORITY FOR COVERING COSTS FOR TREATING QUALIFYING INJURIES UNDER EXTRAORDINARY CIRCUMSTANCES.—Subsection (c) of section 19A of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b) is amended—

(1) by striking ''The Director may'' and inserting the following:

''(1) IN GENERAL.—The Director may''; and

(2) by adding at the end the following:

''(2) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Director deter-

mines extraordinary, the Director may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by a provision of Federal law, regardless of the date of the injury and the location of the employee, individual, or dependent when the injury occurred.''.

(b) ADDITIONAL AUTHORITY FOR MAKING PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN UNDER EXTRAORDINARY CIRCUMSTANCES.—Subsection (d)(2) of such section is amended—

(1) by striking ''Notwithstanding'' and inserting the following:

''(A) IN GENERAL.—Notwithstanding''; and

(2) by adding at the end the following:

''(B) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Director determines extraordinary, the Director may provide payment to a covered employee, a covered individual, or a covered dependent for any qualifying injury to the brain, regardless of the date of the injury and the location of the em-

ployee, individual, or dependent when the injury occurred.''.

(c) CONGRESSIONAL NOTIFICATION.—Such section is amended by adding at the end the following new subsection:

''(e) CONGRESSIONAL NOTIFICATION.—Whenever the Director makes a payment or reimbursement made under subsection (c) or (d)(2), the Director shall, not later than 30 days after the date on which the payment or reimbursement is made, submit to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) a notification of such payment or reimbursement.''.

SEC. 902. ADDITIONAL DISCRETION FOR SECRETARY OF STATE AND HEADS OF OTHER FEDERAL AGENCIES IN PAYING COSTS OF TREATING QUALIFYING INJURIES AND MAKING PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.

(a) ADDITIONAL AUTHORITY FOR COVERING COSTS FOR TREATING QUALIFYING INJURIES UNDER EXTRAORDINARY CIRCUMSTANCES.—Subsection (b) of section 901 of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b) is amended to read as follows:

"(b) COSTS FOR TREATING QUALIFYING INJURIES.—

"(1) IN GENERAL.—The Secretary of State or the head of any other Federal agency may pay or reimburse the costs relating to diagnosing and treating—

"(A) a qualifying injury of a covered employee for such costs, that are not otherwise covered by chapter 81 of title 5, United States Code, or other provision of Federal law; or

"(B) a qualifying injury of a covered individual, or a covered dependent, for such costs that are not otherwise covered by Federal law.

"(2) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Secretary of State or other agency head determines extraordinary, the Secretary or other agency head may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by a provision of Federal law, regardless of the date on which the injury occurred.".

(b) ADDITIONAL AUTHORITY FOR MAKING PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN UNDER

EXTRAORDINARY CIRCUMSTANCES.—Subsection (i)(2) of such section is amended—

(1) by striking ''Notwithstanding'' and inserting the following:

''(A) IN GENERAL.—Notwithstanding''; and

(2) by adding at the end the following:

''(B) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Secretary of State or other agency head with an employee determines extraordinary, the Secretary or other agency head may provide payment to a covered dependent, a dependent of a former employee, a covered employee, a former employee, and a covered individual for any qualifying injury to the brain, regardless of the date on which the injury occurred.''.

(c) CHANGES TO DEFINITIONS.—Subsection (e) of such section is amended—

(1) in paragraph (1)—

(A) in the matter before subparagraph (A), by striking ''a employee who, on or after January 1, 2016'' and inserting ''an employee who, on or after September 11, 2001''; and

(B) in subparagraph (A), by inserting ", or duty station in the United States" before the semicolon;

(2) in paragraph (2)—

(A) by striking "January 1, 2016" and inserting "September 11, 2001"; and

(B) by inserting ", or duty station in the United States," after "pursuant to subsection (f)";

(3) in paragraph (3)—

(A) in the matter before subparagraph (A), by striking "January 1, 2016" and inserting "September 11, 2001"; and

(B) in subparagraph (A), by inserting ", or duty station in the United States" before the semicolon; and

(4) in paragraph (4)—

(A) in subparagraph (A)(i), by inserting ", or duty station in the United States" before the semicolon; and

(B) in subparagraph (B)(i), by inserting ", or duty station in the United States" before the semicolon.

(d) CLARIFICATION RELATING TO AUTHORITIES OF DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY.—

Such section is further amended by adding at the end the following:

''(k) RELATION TO DIRECTOR OF CENTRAL INTELLIGENCE AGENCY.—The authorities and requirements of this section shall not apply to the Director of the Central Intelligence Agency.''.

SEC. 903. IMPROVED FUNDING FLEXIBILITY FOR PAYMENTS MADE BY DEPARTMENT OF STATE FOR QUALIFYING INJURIES TO THE BRAIN.

Section 901(i) of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b) is amended by striking paragraph (3) and inserting the following:

''(3) FUNDING.—

''(A) IN GENERAL.—Payment under paragraph (2) in a fiscal year may be made using any funds—

''(i) appropriated specifically for payments under such paragraph; or

''(ii) reprogrammed in accordance with an applicable provision of law.

''(B) BUDGET.—For each fiscal year, the Secretary of State shall include with the budget justification materials submitted to Congress in support of the budget of the President for that

fiscal year pursuant to section 1105(a) of title 31, United States Code, an estimate of the funds required in that fiscal year to make payments under paragraph (2).''.

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

SEC. 1001. COMPTROLLER GENERAL OF THE UNITED STATES REVIEW OF ALL-DOMAIN ANOMALY RESOLUTION OFFICE.

(a) DEFINITIONS.—In this section, the terms ''congressional defense committees'', ''congressional leadership'', and ''unidentified anomalous phenomena'' have the meanings given such terms in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)).

(b) REVIEW REQUIRED.—The Comptroller General of the United States shall conduct a review of the All-domain Anomaly Resolution Office (in this section referred to as the ''Office'').

(c) ELEMENTS.—The review conducted pursuant to subsection (b) shall include the following:

(1) A review of the implementation by the Office of the duties and requirements of the Office under section 1683 of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373),

such as the process for operational unidentified anomalous phenomena reporting and coordination with the Department of Defense, the intelligence community, and other departments and agencies of the Federal Government and non-Government entities.

(2) A review of such other matters relating to the activities of the Office that pertain to unidentified anomalous phenomena as the Comptroller General considers appropriate.

(d) REPORT.—Following the review required by subsection (b), in a timeframe mutually agreed upon by the congressional intelligence committees, the congressional defense committees, congressional leadership, and the Comptroller General, the Comptroller General shall submit to such committees and congressional leadership a report on the findings of the Comptroller General with respect to the review conducted under subsection (b).

SEC. 1002. SUNSET OF REQUIREMENTS RELATING TO AUDITS OF UNIDENTIFIED ANOMALOUS PHENOMENA HISTORICAL RECORD REPORT.

Section 6001 of the Intelligence Authorization Act for Fiscal Year 2023 (50 U.S.C. 3373 note) is amended—

(1) in subsection (b)(2), by inserting ''until April 1, 2025'' after ''quarterly basis''; and

(2) in subsection (c), by inserting ''until June 30, 2025'' after ''semiannually thereafter''.

SEC. 1003. FUNDING LIMITATIONS RELATING TO UNIDENTIFIED ANOMALOUS PHENOMENA.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Appropriations of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Appropriations of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term ''congressional leadership'' means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(3) UNIDENTIFIED ANOMALOUS PHENOMENA.—The term ''unidentified anomalous phenomena'' has the meaning given such term in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)).

(b) LIMITATIONS.—None of the funds authorized to be appropriated or otherwise made available by this Act may be obligated or expended in support of any activity involving unidentified anomalous phenomena protected under any form of special access or restricted access limitation unless the Director of National Intelligence has provided the details of the activity to the appropriate committees of Congress and congressional leadership, including for any activities described in a report released by the All-domain Anomaly Resolution Office in fiscal year 2024.

(c) LIMITATION REGARDING INDEPENDENT RESEARCH AND DEVELOPMENT.—Independent research and development funding relating to unidentified anomalous phenomena shall not be allowable as indirect expenses for purposes of contracts covered by such instruction, unless such material and information is made available to the appropriate congressional committees and leadership.

TITLE XI—AIR AMERICA

SEC. 1101. SHORT TITLE.

This title may be cited as the ''Air America Act of 2024''.

SEC. 1102. FINDINGS.

Congress finds the following:

(1) Air America and its affiliated companies, in coordination with the Central Intelligence Agency, provided direct and indirect support to the United States Government from 1950 to 1976.

(2) The service and sacrifice of employees of Air America included—

(A) suffering a high rate of casualties in the course of service;

(B) saving thousands of lives in search and rescue missions for downed United States airmen and in allied refugee evacuations; and

(C) serving lengthy periods under challenging circumstances abroad.

SEC. 1103. DEFINITIONS.

In this title:

(1) AFFILIATED COMPANY.—The term ''affiliated company'', with respect to Air America, includes Air Asia Company Limited, CAT Incor-

porated, Civil Air Transport Company Limited, and the Pacific Division of Southern Air Transport.

(2) AIR AMERICA.—The term ''Air America'' means Air America, Incorporated.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(B) the Committee on Oversight and Accountability, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(4) CHILD; DEPENDENT; WIDOW; WIDOWER.—The terms ''child'', ''dependent'', ''widow'', and ''widower'' have the meanings given those terms in section 8341(a) of title 5, United States Code, except that such section shall be applied by substituting ''individual who performed qualifying service'' for ''employee or Member''.

(5) COVERED DECEDENT.—The term ''covered decedent'' means an individual who was killed in Southeast Asia while supporting operations of the

Central Intelligence Agency during the period beginning on January 1, 1950, and ending on December 31, 1976, as a United States citizen employee of Air America or an affiliated company.

(6) DIRECTOR.—The term ''Director'' means the Director of the Central Intelligence Agency.

(7) QUALIFYING SERVICE.— The term ''qualifying service'' means service that—

(A) was performed by a United States citizen as an employee of Air America or an affiliated company during the period beginning on January 1, 1950, and ending on December 31, 1976; and

(B) is documented in—

(i) the corporate records of Air America or an affiliated company;

(ii) records possessed by the United States Government; or

(iii) the personal records of a former employee of Air America or an affiliated company that are verified by the United States Government.

(8) SURVIVOR.—The term ''survivor'' means—

(A) the widow or widower of—

(i) an individual who performed qualifying service; or

(ii) a covered decedent; or

(B) an individual who, at any time during or since the period of qualifying service, or on the date of death of a covered decedent, was a dependent or child of—

(i) the individual who performed such qualifying service; or

(ii) the covered decedent.

SEC. 1104. AWARD AUTHORIZED TO ELIGIBLE PERSONS.

(a) IN GENERAL.—Subject to the limitation in subsection (d), the Director shall provide an award payment of $40,000 under this section—

(1) to an individual who performed qualifying service for a period greater than or equal to 5 years or to a survivor of such individual; or

(2) to the survivor of a covered decedent.

(b) REQUIREMENTS.—

(1) IN GENERAL.—To be eligible for a payment under this subsection, an individual who performed qualifying service or survivor (as the case may be) must demonstrate to the satisfaction of the Director that the individual whose qualifying service upon

which the payment is based meets the criteria of paragraph (1) or (2) of subsection (a).

(2) RELIANCE ON RECORDS.—In carrying out this subsection, in addition to any evidence provided by such an individual or survivor, the Director may rely on records possessed by the United States Government.

(c) ADDITIONAL PAYMENT.—If an individual, or in the case of a survivor, the individual whose qualifying service upon which the payment is based, can demonstrate to the Director that the qualifying service of the individual exceeded 5 years, the Director shall pay to such individual or survivor an additional $8,000 for each full year in excess of 5 years (and a proportionate amount for a partial year).

(d) SURVIVORS.—In the case of an award granted to a survivor under this section, the payment shall be made—

(1) to the surviving widow or widower; or

(2) if there is no surviving widow or widower, to the surviving dependents or children, in equal shares.

SEC. 1105. FUNDING LIMITATION.

(a) IN GENERAL.—The total amount of awards granted under this title may not exceed $60,000,000.

(b) REQUESTS FOR ADDITIONAL FUNDS.—If, at the determination of the Director, the amount of funds required to satisfy all valid applications for payment under this title exceeds the limitation set forth in subsection (a), the Director shall submit to Congress a request for sufficient funds to fulfill all remaining payments.

(c) AWARDS TO EMPLOYEES OF INTERMOUNTAIN AVIATION.—The Director may determine, on a case-by-case basis, to award amounts to individuals who performed service consistent with the definition of qualifying service as employees of Intermountain Aviation.

SEC. 1106. TIME LIMITATION.

(a) IN GENERAL.—To be eligible for an award payment under this title, a claimant must file a claim for such payment with the Director not later than 2 years after the effective date of the regulations prescribed by the Director in accordance with section 1107.

(b) DETERMINATION.—Not later than 90 days after receiving a claim for an award payment under this section, the Director shall determine the eligibility of the claimant for payment.

(c) PAYMENT.—

(1) IN GENERAL.—If the Director determines that the claimant is eligible for the award payment,

the Director shall pay the award payment not later than 60 days after the date of such determination.

(2) LUMP-SUM PAYMENT.—The Director shall issue each payment as a one-time lump sum payment contingent upon the timely filing of the claimant under this section.

(3) NOTICE AND DELAYS.—The Director shall notify the appropriate congressional committees of any delays in making an award payment not later than 30 days after the date such payment is due.

SEC. 1107. APPLICATION PROCEDURES.

(a) IN GENERAL.—The Director shall prescribe procedures to carry out this title, which shall include processes under which—

(1) claimants may submit claims for payment under this title;

(2) the Director will award the amounts under section 1104; and

(3) claimants can obtain redress and appeal determinations under section 1106.

(b) OTHER MATTERS.—Such procedures—

(1) shall be—

(A) prescribed not later than 60 days after the date of the enactment of this Act; and

(B) published in the Code of Federal Regulations; and

(2) shall not be subject to chapter 5 of title 5, United States Code.

SEC. 1108. RULE OF CONSTRUCTION.

Nothing in this title shall be construed to—

(1) entitle any person to Federal benefits, including retirement benefits under chapter 83 or 84 of title 5, United States Code, and disability or death benefits under chapter 81 of such title;

(2) change the legal status of the former Air America corporation or any affiliated company; or

(3) create any legal rights, benefits, or entitlements beyond the one-time award authorized by this title.

SEC. 1109. ATTORNEYS' AND AGENTS' FEES.

(a) IN GENERAL.—It shall be unlawful for more than 25 percent of an award paid pursuant to this title to be paid to, or received by, any agent or attorney for any service rendered to a person who receives an award under section 1104, in connection with the award under this title.

(b) VIOLATION.—Any agent or attorney who violates subsection (a) shall be fined under title 18, United States Code.

SEC. 1110. NO JUDICIAL REVIEW.

A determination by the Director pursuant to this title is final and conclusive and shall not be subject to judicial review.

SEC. 1111. REPORTS TO CONGRESS.

Until the date that all funds available for awards under this title are expended, the Director shall submit to the appropriate congressional committees a semiannual report describing the number of award payments made and denied during the 180 days preceding the submission of the report, including the rationales for any denials, and if, at the determination of the Director, the amount of funds provided to carry out this title is insufficient to satisfy any remaining or anticipated claims.

TITLE XII—OTHER MATTERS

SEC. 1201. ENHANCED AUTHORITIES FOR AMICUS CURIAE UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) EXPANSION OF APPOINTMENT AUTHORITY.—

(1) IN GENERAL.—Section 103(i)(2)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)(A)) is amended by striking clause (i) and inserting the following:

"(i) shall appoint one or more individuals who have been designated under paragraph (1), not less than one of whom pos-

sesses privacy and civil liberties expertise, unless the court finds that such a qualification is inappropriate, to serve as amicus curiae to assist the court in the consideration of any application or motion for an order or review that, in the opinion of the court—

"(I) presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate;

"(II) presents exceptional concerns with respect to the activities of a United States person that are protected by the first amendment to the Constitution of the United States, unless the court issues a finding that such appointment is not appropriate;

"(III) targets a United States person and presents or involves a sensitive investigative matter, unless—

"(aa) the matter represents an immediate danger to human life; or

"(bb) the court issues a finding that such appointment is not appropriate;

"(IV) targets a United States person and presents a request for approval of programmatic surveillance or reauthorization of programmatic surveillance, unless the court issues a finding that such appointment is not appropriate; or

"(V) targets a United States person and otherwise presents novel or exceptional civil liberties issues, unless the court issues a finding that such appointment is not appropriate;".

(2) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—Subsection (i) of section 103 of such Act (50 U.S.C. 1803) is amended by adding at the end the following:

"(12) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—In this subsection, the term 'sensitive investigative matter' means—

"(A) an investigative matter that targets a United States person who is—

"(i) a United States elected official;

"(ii) an appointee of—

"(I) the President; or

"(II) a State Governor;

"(iii) a United States political candidate;

"(iv) a United States political organization or an individual prominent in such an organization;

"(v) a United States news media organization or a member of a United States news media organization; or

"(vi) a United States religious organization or an individual prominent in such an organization; or

"(B) any other investigative matter involving a domestic entity or a known or presumed United States person that, in the judgment of the applicable court established under subsection (a) or (b), is as sensitive as an investigative matter described in subparagraph (A).".

(b) AUTHORITY TO SEEK REVIEW.—Subsection (i) of such section (50 U.S.C. 1803), as amended by subsection (a) of this section, is further amended—

(1) in paragraph (4)—

(A) in the paragraph heading, by inserting ''; AUTHORITY'' after ''DUTIES'';

(B) by striking ''the amicus curiae shall'' and all that follows through ''provide'' and insert the following: ''the amicus curiae—

''(A) shall provide'';

(C) in subparagraph (A), as so designated—

(i) in clause (i), by inserting before the semicolon at the end the following: '', including legal arguments regarding any privacy or civil liberties interest of any United States person that would be significantly impacted by the application or motion''; and

(ii) in clause (iii), by striking the period at the end and inserting ''; and''; and

(D) by adding at the end the following:

''(B) may seek leave to raise any novel or significant privacy or civil liberties issue relevant to the application or motion or other issue directly impacting the legality of the proposed electronic surveillance with the court, regardless of whether the court has requested assistance on that issue.'';

(2) by redesignating paragraphs (7) through (12) as paragraphs (8) through (13), respectively; and

(3) by inserting after paragraph (6) the following:

''(7) AUTHORITY TO SEEK REVIEW OF DECISIONS.—

''(A) FISA COURT DECISIONS.—Following issuance of a final order under this Act by the Foreign Intelligence Surveillance Court in a matter in which an amicus curiae was appointed under paragraph (2), that amicus curiae may petition the Foreign Intelligence Surveillance Court to certify for review to the Foreign Intelligence Surveillance Court of Review a question of law pursuant to subsection (j). If the court denies such petition, the court shall provide for the record a written statement of the reasons for such denial. Upon certification of any question of law pursuant to this subparagraph, the Court of Review shall appoint the amicus curiae to assist the Court of Review in its consideration of the certified question, unless the Court of Review issues a finding that such appointment is not appropriate.

"(B) FISA COURT OF REVIEW DECISIONS.—An amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court of Review to certify for review to the Supreme Court of the United States any question of law pursuant to section 1254(2) of title 28, United States Code, in the matter in which that amicus curiae was appointed.

"(C) DECLASSIFICATION OF REFERRALS.—For purposes of section 602, if the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review denies a petition filed under subparagraph (A) or (B) of this paragraph, that petition and all of its content shall be considered a decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review described in section 602(a).".

(c) ACCESS TO INFORMATION.—

(1) APPLICATION AND MATERIALS.—Subparagraph (A) of section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is amended to read as follows:

"(A) IN GENERAL.—

"(i) RIGHTS OF AMICUS.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

"(I) shall have access to, to the extent such information is available to the Government and the court established under subsection (a) or (b) determines it is necessary to fulfill the duties of the amicus curiae—

"(aa) the application, certification, petition, motion, and other information and supporting materials submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed, including access to any relevant legal precedent (including any such precedent that is cited by the Government, including in such an application);

"(bb) a copy of each relevant decision made by the For-

eign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review in which the court decides a question of law, without regard to whether the decision is classified; and

"(cc) any other information or materials that the court determines are relevant to the duties of the amicus curiae; and

"(II) may make a submission to the court requesting access to any other particular materials or information (or category of materials or information) that the amicus curiae believes to be relevant to the duties of the amicus curiae.

"(ii) SUPPORTING DOCUMENTATION REGARDING ACCURACY.—The Foreign Intelligence Surveillance Court, upon the motion of an amicus curiae appointed under paragraph (2) or upon its own motion, may require the Government to make available the supporting documentation re-

garding the accuracy of any material submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed if the court determines the information is relevant to the duties of the amicus curiae.''.

(2) CLARIFICATION OF ACCESS TO CERTAIN INFORMATION.—Such section is further amended by striking subparagraph (C) and inserting the following:

''(C) CLASSIFIED INFORMATION.—An amicus curiae appointed by the court shall have access, to the extent such information is available to the Government and the court determines such information is relevant to the duties of the amicus curiae in the matter in which the amicus curiae was appointed, to copies of each opinion, order, transcript, pleading, or other document of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review, including, if the individual is eligible for access to classified information, any classified documents, information, and other materials or proceedings, but only to the

extent consistent with the national security of the United States.''.

(3) CONSULTATION AMONG AMICI CURIAE.—Such section is further amended—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

(B) by inserting after subparagraph (A) the following:

''(B) CONSULTATION.—If the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review determines that it is relevant to the duties of an amicus curiae appointed by the court under paragraph (2), the amicus curiae may consult with one or more of the other individuals designated to serve as amicus curiae pursuant to paragraph (1) regarding any of the information relevant to any assigned proceeding.''.

(d) TERM LIMITS.—

(1) REQUIREMENT.—Paragraph (1) of section 103(i) of such Act (50 U.S.C. 1803(i)) is amended by adding at the end the following new sentence: ''An individual may serve as an amicus curiae for a 5-year term, and the presiding judges may, for good

cause, jointly reappoint the individual to a single additional 5-year term.''.

(2) APPLICATION.—The amendment made by paragraph (1) shall apply with respect to the service of an amicus curiae appointed under section 103(i) of such Act (50 U.S.C. 1803(i)) that occurs on or after the date of the enactment of this Act, regardless of the date on which the amicus curiae is appointed.

SEC. 1202. LIMITATION ON DIRECTIVES UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 RELATING TO CERTAIN ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

Section 702(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(i)) is amended by adding at the end the following:

''(7) LIMITATION RELATING TO CERTAIN ELECTRONIC COMMUNICATION SERVICE PROVIDERS.—

''(A) DEFINITIONS.—In this paragraph:

''(i) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' means—

''(I) the congressional intelligence committees;

"(II) the Committee on the Judiciary of the Senate; and

"(III) the Committee on the Judiciary of the House of Representatives.

"(ii) COVERED ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'covered electronic communication service provider' means—

"(I) a service provider described in section 701(b)(4)(E); or

"(II) a custodian of an entity as defined in section 701(b)(4)(F).

"(iii) COVERED OPINIONS.—The term 'covered opinions' means the opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review authorized for public release on August 23, 2023 (Opinion and Order, In re Petition to Set Aside or Modify Directive Issued to [REDACTED], No. [REDACTED], (FISA Ct. [REDACTED] 2022) (Contreras J.); Opinion, In re Petition to Set Aside or Modify Directive Issued to [REDACTED], No. [RE-

DACTED], (FISA Ct. Rev. [REDACTED] 2023) (Sentelle, J.; Higginson, J.; Miller J.)).

''(B) LIMITATION.—A directive may not be issued under paragraph (1) to a covered electronic communication service provider unless the covered electronic communication service provider is a provider of the type of service at issue in the covered opinions.

''(C) REQUIREMENTS FOR DIRECTIVES TO COVERED ELECTRONIC COMMUNICATION SERVICE PROVIDERS.—

''(i) IN GENERAL.—Subject to clause (ii), any directive issued under paragraph (1) on or after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 to a covered electronic communication service provider that is not prohibited by subparagraph (B) of this paragraph shall include a summary description of the services at issue in the covered opinions.

''(ii) DUPLICATE SUMMARIES NOT REQUIRED.—A directive need not include a summary description of the services at

issue in the covered opinions if such summary was included in a prior directive issued to the covered electronic communication service provider and the summary has not materially changed.

"(D) FOREIGN INTELLIGENCE SURVEILLANCE COURT NOTIFICATION AND REVIEW.—

"(i) NOTIFICATION.—

"(I) IN GENERAL.—Subject to subclause (II), each time the Attorney General and the Director of National Intelligence issue a directive under paragraph (1) to a covered electronic communication service provider that is not prohibited by subparagraph (B) and each time the Attorney General and the Director materially change a directive under paragraph (1) issued to a covered electronic communication service provider that is not prohibited by subparagraph (B), the Attorney General and the Director shall provide the directive to the Foreign Intelligence Surveillance Court on or before the date that is 7 days after the

date on which the Attorney General and the Director issue the directive, along with a description of the covered electronic communication service provider to whom the directive is issued and the services at issue.

"(II) DUPLICATION NOT REQUIRED.—The Attorney General and the Director do not need to provide a directive or description to the Foreign Intelligence Surveillance Court under subclause (I) if a directive and description concerning the covered electronic communication service provider was previously provided to the Court and the directive or description has not materially changed.

"(ii) ADDITIONAL INFORMATION.—As soon as feasible and not later than the initiation of collection, the Attorney General and the Director shall, for each directive described in subparagraph (i), provide the Foreign Intelligence Surveillance Court a description of the type of equipment to be accessed, the nature of the access, and the

form of assistance required pursuant to the directive.

"(iii) REVIEW.—

"(I) IN GENERAL.—The Foreign Intelligence Surveillance Act Court may review a directive received by the Court under clause (i) to determine whether the directive is consistent with subparagraph (B) and affirm, modify, or set aside the directive.

"(II) NOTICE OF INTENT TO REVIEW.—Not later than 10 days after the date on which the Court receives information under clause (ii) with respect to a directive, the Court shall provide notice to the Attorney General, the Director, and the covered electronic communication service provider, indicating whether the Court intends to undertake a review under subclause (I) of this clause.

"(III) COMPLETION OF REVIEWS.—In a case in which the Court provides notice under subclause (II) indicating that the Court intends to

review a directive under subclause (I), the Court shall, not later than 30 days after the date on which the Court provides notice under subclause (II) with respect to the directive, complete the review.

''(E) CONGRESSIONAL OVERSIGHT.—

''(i) NOTIFICATION.—

''(I) IN GENERAL.—Subject to subclause (II), each time the Attorney General and the Director of National Intelligence issue a directive under paragraph (1) to a covered electronic communication service provider that is not prohibited by subparagraph (B) and each time the Attorney General and the Director materially change a directive under paragraph (1) issued to a covered electronic communication service provider that is not prohibited by subparagraph (B), the Attorney General and the Director shall submit to the appropriate committees of Congress the directive on or before the date that is 7 days after the date on

which the Attorney General and the Director issue the directive, along with description of the covered electronic communication service provider to whom the directive is issued and the services at issue.

"(II) DUPLICATION NOT REQUIRED.—The Attorney General and the Director do not need to submit a directive or description to the appropriate committees of Congress under subclause (I) if a directive and description concerning the covered electronic communication service provider was previously submitted to the appropriate committees of Congress and the directive or description has not materially changed.

"(ii) ADDITIONAL INFORMATION.—As soon as feasible and not later than the initiation of collection, the Attorney General and the Director shall, for each directive described in subparagraph (i), provide the appropriate committees of Congress a description of the type of equipment to be

accessed, the nature of the access, and the form of assistance required pursuant to the directive.

"(iii) REPORTING.—

"(I) QUARTERLY REPORTS.—Not later than 90 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 and not less frequently than once each quarter thereafter, the Attorney General and the Director shall submit to the appropriate committees of Congress a report on the number of directives issued, during the period covered by the report, under paragraph (1) to a covered electronic communication service provider and the number of directives provided during the same period to the Foreign Intelligence Surveillance Court under subparagraph (D)(i).

"(II) FORM OF REPORTS.—Each report submitted pursuant to subclause (I) shall be submitted in un-

classified form, but may include a classified annex.

''(III) SUBMITTAL OF COURT OPINIONS.—Not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues an opinion relating to a directive issued to a covered electronic communication service provider under paragraph (1), the Attorney General shall submit to the appropriate committees of Congress a copy of the opinion.''.

SEC. 1203. STRENGTHENING ELECTION CYBERSECURITY TO UPHOLD RESPECT FOR ELECTIONS THROUGH INDEPENDENT TESTING ACT OF 2024.

(a) SHORT TITLE.—This section may be cited as the ''Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024'' or the ''SECURE IT Act of 2024''.

(b) REQUIRING PENETRATION TESTING AS PART OF THE TESTING AND CERTIFICATION OF VOTING SYSTEMS.—Section 231 of the Help America Vote Act of

2002 (52 U.S.C. 20971) is amended by adding at the end the following new subsection:

''(e) REQUIRED PENETRATION TESTING.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Commission shall provide for the conduct of penetration testing as part of the testing, certification, decertification, and recertification of voting system hardware and software by the Commission based on accredited laboratories under this section.

''(2) ACCREDITATION.—The Commission shall develop a program for the acceptance of the results of penetration testing on election systems. The penetration testing required by this subsection shall be required for Commission certification. The Commission shall vote on the selection of any entity identified. The requirements for such selection shall be based on consideration of an entity's competence to conduct penetration testing under this subsection. The Commission may consult with the National Institute of Standards and Technology or any other appropriate Federal agency on lab selection criteria and other aspects of this program.''.

(c) INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS.—

(1) IN GENERAL.—Subtitle D of title II of the Help America Vote Act of 2002 (42 U.S.C. 15401 et seq.) is amended by adding at the end the following new part:

"PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS

"SEC. 297. INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS.

''(a) IN GENERAL.—

''(1) ESTABLISHMENT.—The Commission, in consultation with the Secretary, shall establish an Independent Security Testing and Coordinated Vulnerability Disclosure Pilot Program for Election Systems (VDP–E) (in this section referred to as the 'program') to test for and disclose cybersecurity vulnerabilities in election systems.

''(2) DURATION.—The program shall be conducted for a period of 5 years.

"(3) REQUIREMENTS.—In carrying out the program, the Commission, in consultation with the Secretary, shall—

"(A) establish a mechanism by which an election systems vendor may make their election system (including voting machines and source code) available to cybersecurity researchers participating in the program;

"(B) provide for the vetting of cybersecurity researchers prior to their participation in the program, including the conduct of background checks;

"(C) establish terms of participation that—

"(i) describe the scope of testing permitted under the program;

"(ii) require researchers to—

"(I) notify the vendor, the Commission, and the Secretary of any cybersecurity vulnerability they identify with respect to an election system; and

"(II) otherwise keep such vulnerability confidential for 180 days after such notification;

"(iii) require the good faith participation of all participants in the program;

"(iv) require an election system vendor, within 180 days after validating notification of a critical or high vulnerability (as defined by the National Institute of Standards and Technology) in an election system of the vendor, to—

"(I) send a patch or propound some other fix or mitigation for such vulnerability to the appropriate State and local election officials, in consultation with the researcher who discovered it; and

"(II) notify the Commission and the Secretary that such patch has been sent to such officials;

"(D) in the case where a patch or fix to address a vulnerability disclosed under subparagraph (C)(ii)(I) is intended to be applied to a system certified by the Commission, provide—

"(i) for the expedited review of such patch or fix within 90 days after receipt by the Commission; and

"(ii) if such review is not completed by the last day of such 90-day period, that such patch or fix shall be deemed to be certified by the Commission, subject to any subsequent review of such determination by the Commission; and

"(E) 180 days after the disclosure of a vulnerability under subparagraph (C)(ii)(I), notify the Director of the Cybersecurity and Infrastructure Security Agency of the vulnerability for inclusion in the database of Common Vulnerabilities and Exposures.

"(4) VOLUNTARY PARTICIPATION; SAFE HARBOR.—

"(A) VOLUNTARY PARTICIPATION.—Participation in the program shall be voluntary for election systems vendors and researchers.

"(B) SAFE HARBOR.—When conducting research under this program, such research and subsequent publication shall be—

"(i) authorized in accordance with section 1030 of title 18, United States Code (commonly known as the 'Computer Fraud and Abuse Act'), (and similar State laws), and the election system vendor will

not initiate or support legal action against the researcher for accidental, good faith violations of the program; and

''(ii) exempt from the anti-circumvention rule of section 1201 of title 17, United States Code (commonly known as the 'Digital Millennium Copyright Act'), and the election system vendor will not bring a claim against a researcher for circumvention of technology controls.

''(C) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to limit or otherwise affect any exception to the general prohibition against the circumvention of technological measures under subparagraph (A) of section 1201(a)(1) of title 17, United States Code, including with respect to any use that is excepted from that general prohibition by the Librarian of Congress under subparagraphs (B) through (D) of such section 1201(a)(1).

''(5) DEFINITIONS.—In this subsection:

''(A) CYBERSECURITY VULNERABILITY.—The term 'cybersecurity vulnerability' means, with respect to an election system, any security vulnerability that affects the election system.

"(B) ELECTION INFRASTRUCTURE.—The term 'election infrastructure' means—

"(i) storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office; and

"(ii) related information and communications technology, including—

"(I) voter registration databases;

"(II) election management systems;

"(III) voting machines;

"(IV) electronic mail and other communications systems (including electronic mail and other systems of vendors who have entered into contracts with election agencies to support the administration of elections, manage the election process, and report and display election results); and

"(V) other systems used to manage the election process and to report and display election results on behalf of an election agency.

"(C) ELECTION SYSTEM.—The term 'election system' means any information system that is part of an election infrastructure, including any related information and communications technology described in subparagraph (B)(ii).

"(D) ELECTION SYSTEM VENDOR.—The term 'election system vendor' means any person providing, supporting, or maintaining an election system on behalf of a State or local election official.

"(E) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

"(F) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"(G) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end

of the items relating to subtitle D of title II the following:

"PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS

"Sec. 297. Independent security testing and coordinated cybersecurity vulnerability disclosure program for election systems.".

SEC. 1204. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD QUALIFICATIONS.

Section 1061(h)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(h)(2)) is amended by striking "and relevant experience" and inserting "or experience in positions requiring a security clearance, and relevant national security experience".

SEC. 1205. PARITY IN PAY FOR STAFF OF THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE INTELLIGENCE COMMUNITY.

Section 1061(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(j)(1)) is amended by striking "except that" and all that follows through the period at the end and inserting "except that no rate of pay fixed under this subsection may exceed the highest amount paid by any element of the intelligence community for a comparable position, based on salary information provided to the chairman of the Board by the Director of National Intelligence.".

SEC. 1206. MODIFICATION AND REPEAL OF REPORTING REQUIREMENTS.

(a) BRIEFING ON IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.—Section 6705(a)(1) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412(a)(1)) is amended by striking ", and not less frequently than once each year thereafter provide a briefing to Congress,".

(b) REPORTS AND BRIEFINGS ON NATIONAL SECURITY EFFECTS OF GLOBAL WATER INSECURITY AND EMERGING INFECTIOUS DISEASES AND PANDEMICS.—Section 6722(b) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3024 note; division E of Public Law 116–92) is amended by—

(1) striking paragraph (2); and

(2) redesignating paragraphs (3) and (4) as paragraphs (2) and (3), respectively.

(c) REPEAL OF REPORT ON REMOVAL OF SATELLITES AND RELATED ITEMS FROM THE UNITED STATES MUNITIONS LIST.—Section 1261(e) of the National Defense Authorization Act for Fiscal Year 2013 (22 U.S.C. 2778 note; Public Law 112–239) is repealed.

(d) BRIEFING ON REVIEW OF INTELLIGENCE COMMUNITY ANALYTIC PRODUCTION.—Section 1019(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3364(c)) is amended by striking ''December 1'' and inserting ''February 1''.

(e) REPEAL OF REPORT ON OVERSIGHT OF FOREIGN INFLUENCE IN ACADEMIA.—Section 5713 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3369b) is repealed.

(f) REPEAL OF BRIEFING ON IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.—Section 6705 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) is amended—

(1) by striking subsection (b);

(2) by striking the enumerator and heading for subsection (a);

(3) by redesignating paragraphs (1) and (2) as subsections (a) and (b), respectively, and moving such subsections, as so redesignated, 2 ems to the left;

(4) in subsection (a), as so redesignated, by redesignating subparagraphs (A) and (B) as para-

graphs (1) and (2), respectively, and moving such paragraphs, as so redesignated, 2 ems to the left; and

(5) in paragraph (1), as so redesignated, by redesignating clauses (i) through (v) as subparagraphs (A) through (E), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the left.

(g) REPEAL OF REPORT ON FOREIGN INVESTMENT RISKS.—Section 6716 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3370a) is repealed.

(h) REPEAL OF REPORT ON INTELLIGENCE COMMUNITY LOAN REPAYMENT PROGRAMS.—Section 6725(c) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334g(c)) is repealed.

(i) REPEAL OF REPORT ON DATA COLLECTION ON ATTRITION IN INTELLIGENCE COMMUNITY.—Section 306(c) of the Intelligence Authorization Act for Fiscal Year 2021 (50 U.S.C. 3334h(c)) is repealed.

SEC. 1207. TECHNICAL AMENDMENTS.

(a) REQUIREMENTS RELATING TO CONSTRUCTION OF FACILITIES TO BE USED PRIMARILY BY INTELLIGENCE COMMUNITY.—Section 602(a) of the Intelligence

Authorization Act for Fiscal Year 1995 (50 U.S.C. 3304(a)) is amended—

(1) in paragraph (1), by striking ''$6,000,000'' and inserting ''$9,000,000''; and

(2) in paragraph (2)—

(A) by striking ''$2,000,000'' each place it appears and inserting ''$4,000,000''; and

(B) by striking ''$6,000,000'' and inserting ''$9,000,000''.

(b) COPYRIGHT PROTECTION FOR CIVILIAN FACULTY OF CERTAIN ACCREDITED INSTITUTIONS.—Section 105 of title 17, United States Code, is amended to read as follows:

''§ 105. Subject matter of copyright: United States Government works

''(a) IN GENERAL.—Copyright protection under this title is not available for any work of the United States Government, but the United States Government is not precluded from receiving and holding copyrights transferred to it by assignment, bequest, or otherwise.

''(b) COPYRIGHT PROTECTION OF CERTAIN WORKS.—Subject to subsection (c), the covered author of a covered work owns the copyright to that covered work.

''(c) USE BY FEDERAL GOVERNMENT.—

"(1) SECRETARY OF DEFENSE AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at a covered institution described in subparagraphs (A) through (K) of subsection (d)(2), the Secretary of Defense may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

"(2) SECRETARY OF HOMELAND SECURITY AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(L), the Secretary of Homeland Security may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

"(3) DIRECTOR OF NATIONAL INTELLIGENCE AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(M), the Director of National Intel-

ligence may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

''(4) SECRETARY OF TRANSPORTATION AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(N), the Secretary of Transportation may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

''(d) DEFINITIONS.—In this section:

''(1) COVERED AUTHOR.—The term 'covered author' means a civilian member of the faculty of a covered institution.

''(2) COVERED INSTITUTION.—The term 'covered institution' means the following:

''(A) National Defense University.

''(B) United States Military Academy.

''(C) Army War College.

"(D) United States Army Command and General Staff College.

"(E) United States Naval Academy.

"(F) Naval War College.

"(G) Naval Postgraduate School.

"(H) Marine Corps University.

"(I) United States Air Force Academy.

"(J) Air University.

"(K) Defense Language Institute.

"(L) United States Coast Guard Academy.

"(M) National Intelligence University.

"(N) United States Merchant Marine Academy.

"(3) COVERED WORK.—The term 'covered work' means a literary work produced by a covered author in the course of employment at a covered institution for publication by a scholarly press or journal.".

Title: To authorize appropriations for fiscal year 2025 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the "Intelligence Authorization Act for Fiscal Year 2025".

(b) Table of Contents.—The table of contents for this Act is as follows:

Sec.1.Short title; table of contents.
Sec.2.Definitions.
TITLE I—INTELLIGENCE ACTIVITIES
Sec.101.Authorization of appropriations.
Sec.102.Classified Schedule of Authorizations.
Sec.103.Intelligence Community Management Account.
Sec.104.Increase in employee compensation and benefits authorized by law.
TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM
Sec.201.Authorization of appropriations.
TITLE III—INTELLIGENCE COMMUNITY MATTERS
Sec.301.Improvements relating to conflicts of interest in the Intelligence Innovation Board.
Sec.302.National Threat Identification and Prioritization Assessment and National Counterintelligence Strategy.
Sec.303.Open Source Intelligence Division of Office of Intelligence and Analysis personnel.
Sec.304.Appointment of Director of the Office of Intelligence and Counterintelligence.
Sec.305.Improvements to advisory board of National Reconnaissance Office.
Sec.306.National Intelligence University acceptance of grants.
Sec.307.Protection of Central Intelligence Agency facilities and assets from unmanned aircraft.
Sec.308.Limitation on availability of funds for new controlled access programs.
Sec.309.Limitation on transfers from controlled access programs.
Sec.310.Expenditure of funds for certain intelligence and counterintelligence activities of the

Coast Guard.
Sec.311.Unauthorized access to intelligence community property.
Sec.312.Strengthening of Office of Intelligence and Analysis.
Sec.313.Report on sensitive commercially available information.
Sec.314.Policy on collection of United States location information.
Sec.315.Display of flags, seals, and emblems other than the United States flag.
TITLE IV—COUNTERING FOREIGN THREATS
Subtitle A—People's Republic of China
Sec.401.Strategy and outreach on risks posed by People's Republic of China smartport technology.
Sec.402.Assessment of current status of biotechnology of People's Republic of China.
Sec.403.Intelligence sharing with law enforcement agencies on synthetic opioid precursor chemicals originating in People's Republic of China.
Sec.404.Report on efforts of the People's Republic of China to evade United States transparency and national security regulations.
Sec.405.Plan for recruitment of Mandarin speakers.
Subtitle B—The Russian Federation
Sec.411.Assessment of Russian Federation sponsorship of acts of international terrorism.
Sec.412.Assessment of likely course of war in Ukraine.
Subtitle C—International Terrorism
Sec.421.Inclusion of Hamas, Hezbollah, Al-Qaeda, and ISIS officials and members among aliens engaged in terrorist activity.
Sec.422.Assessment and report on the threat of ISIS-Khorasan to the United States.
Sec.423.Terrorist financing prevention.
Subtitle D—Other Foreign Threats
Sec.431.Assessment of visa-free travel to and within Western Hemisphere by nationals of countries of concern.
Sec.432.Study on threat posed by foreign investment in United States agricultural land.
Sec.433.Assessment of threat posed by citizenship-by-investment programs.
Sec.434.Mitigating the use of United States components and technology in hostile activities by foreign adversaries.
Sec.435.Office of Intelligence and Counterintelligence review of visitors and assignees.

Sec.436.Prohibition on National Laboratories admitting certain foreign nationals.

Sec.437.Quarterly report on certain foreign nationals encountered at the United States border.

Sec.438.Assessment of the lessons learned by the intelligence community with respect to the Israel-Hamas war.

Sec.439.Central Intelligence Agency intelligence assessment on Tren de Aragua.

Sec.440.Assessment of Maduro regime's economic and security relationships with state sponsors of terrorism and foreign terrorist organizations.

Sec.441.Continued congressional oversight of Iranian expenditures supporting foreign military and terrorist activities.

TITLE V—EMERGING TECHNOLOGIES

Sec.501.Strategy to counter foreign adversary efforts to utilize biotechnologies in ways that threaten United States national security.

Sec.502.Improvements to the roles, missions, and objectives of the National Counterproliferation and Biosecurity Center.

Sec.503.Enhancing capabilities to detect foreign adversary threats relating to biological data.

Sec.504.National security procedures to address certain risks and threats relating to artificial intelligence.

Sec.505.Establishment of Artificial Intelligence Security Center.

Sec.506.Sense of Congress encouraging intelligence community to increase private sector capital partnerships and partnership with Office of Strategic Capital of Department of Defense to secure enduring technological advantages.

Sec.507.Intelligence Community Technology Bridge Fund.

Sec.508.Enhancement of authority for intelligence community public-private talent exchanges.

Sec.509.Enhancing intelligence community ability to acquire emerging technology that fulfills intelligence community needs.

Sec.510.Management of artificial intelligence security risks.

Sec.511.Protection of technological measures designed to verify authenticity or provenance of machine-manipulated media.

Sec.512.Sense of Congress on hostile foreign cyber actors.

Sec.513.Designation of state sponsors of ransomware and reporting requirements.

Sec.514.Deeming ransomware threats to critical infrastructure a national intelligence priority.

TITLE VI—CLASSIFICATION REFORM

Sec.601.Governance of classification and declassification system.

Sec.602.Classification and declassification of information.

Sec.603.Minimum standards for Executive agency insider threat programs.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

Sec.701.Security clearances held by certain former employees of intelligence community.

Sec.702.Policy for authorizing intelligence community program of contractor-owned and contractor-operated sensitive compartmented information facilities.

Sec.703.Enabling intelligence community integration.

Sec.704.Appointment of spouses of certain Federal employees.

Sec.705.Plan for staffing the intelligence collection positions of the Central Intelligence Agency.

Sec.706.Intelligence community workplace protections.

Sec.707.Sense of Congress on Government personnel support for foreign terrorist organizations.

TITLE VIII—WHISTLEBLOWERS

Sec.801.Improvements regarding urgent concerns submitted to Inspectors General of the intelligence community.

Sec.802.Prohibition against disclosure of whistleblower identity as act of reprisal.

Sec.803.Protection for individuals making authorized disclosures to Inspectors General of elements of the intelligence community.

Sec.804.Clarification of authority of certain Inspectors General to receive protected disclosures.

Sec.805.Whistleblower protections relating to psychiatric testing or examination.

Sec.806.Establishing process parity for adverse security clearance and access determinations.

Sec.807.Elimination of cap on compensatory damages for retaliatory revocation of security clearances and access determinations.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

Sec.901.Additional discretion for Director of Central Intelligence Agency in paying costs of treating qualifying injuries and making payments for qualifying injuries to the brain.

Sec.902.Additional discretion for Secretary of State and heads of other Federal agencies in paying costs of treating qualifying injuries and making payments for qualifying injuries to the brain.

Sec.903.Improved funding flexibility for payments made by Department of State for qualifying injuries to the brain.

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

Sec.1001.Comptroller General of the United States review of All-domain Anomaly Resolution

Office.

Sec.1002.Sunset of requirements relating to audits of unidentified anomalous phenomena historical record report.

Sec.1003.Funding limitations relating to unidentified anomalous phenomena.

TITLE XI—AIR AMERICA

Sec.1101.Short title.

Sec.1102.Findings.

Sec.1103.Definitions.

Sec.1104.Award authorized to eligible persons.

Sec.1105.Funding limitation.

Sec.1106.Time limitation.

Sec.1107.Application procedures.

Sec.1108.Rule of construction.

Sec.1109.Attorneys' and agents' fees.

Sec.1110.No judicial review.

Sec.1111.Reports to Congress.

TITLE XII—OTHER MATTERS

Sec.1201.Enhanced authorities for amicus curiae under the Foreign Intelligence Surveillance Act of 1978.

Sec.1202.Limitation on directives under Foreign Intelligence Surveillance Act of 1978 relating to certain electronic communication service providers.

Sec.1203.Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024.

Sec.1204.Privacy and Civil Liberties Oversight Board qualifications.

Sec.1205.Parity in pay for staff of the Privacy and Civil Liberties Oversight Board and the intelligence community.

Sec.1206.Modification and repeal of reporting requirements.

Sec.1207.Technical amendments.

SEC. 2. DEFINITIONS.

In this Act:

(1) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term "congressional intelligence committees" has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(2) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given such term in such section.

TITLE I—INTELLIGENCE ACTIVITIES

SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

Funds are hereby authorized to be appropriated for fiscal year 2025 for the conduct of the intelligence and intelligence-related activities of the Federal Government.

SEC. 102. CLASSIFIED SCHEDULE OF AUTHORIZATIONS.

(a) Specifications of Amounts.—The amounts authorized to be appropriated under section 101 for the conduct of the intelligence activities of the Federal Government are those specified in the classified Schedule of Authorizations prepared to accompany this Act.

(b) Availability of Classified Schedule of Authorizations.—

(1) AVAILABILITY.—The classified Schedule of Authorizations referred to in subsection (a) shall be made available to the Committee on Appropriations of the Senate, the Committee on Appropriations of the House of Representatives, and to the President.

(2) DISTRIBUTION BY THE PRESIDENT.—Subject to paragraph (3), the President shall provide for suitable distribution of the classified Schedule of Authorizations referred to in subsection (a), or of appropriate portions of such Schedule, within the executive branch of the Federal Government.

(3) LIMITS ON DISCLOSURE.—The President shall not publicly disclose the classified Schedule of Authorizations or any portion of such Schedule except—

(A) as provided in section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 3306(a));

(B) to the extent necessary to implement the budget; or

(C) as otherwise required by law.

SEC. 103. INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT.

(a) Authorization of Appropriations.—There is authorized to be appropriated for the Intelligence Community Management Account of the Director of National Intelligence for fiscal year 2025 the sum of $656,573,000.

(b) Classified Authorization of Appropriations.—In addition to amounts authorized to be appropriated for the Intelligence Community Management Account by subsection (a), there are authorized to be appropriated for the Intelligence Community Management Account for fiscal year 2025 such additional amounts as are specified in the classified Schedule of Authorizations referred to in section 102(a).

SEC. 104. INCREASE IN EMPLOYEE COMPENSATION AND BENEFITS AUTHORIZED BY LAW.

Appropriations authorized by this Act for salary, pay, retirement, and other benefits for Federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in such compensation or benefits authorized by law.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

SEC. 201. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the Central Intelligence Agency Retirement and Disability Fund $514,000,000 for fiscal year 2025.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

SEC. 301. IMPROVEMENTS RELATING TO CONFLICTS OF INTEREST IN THE INTELLIGENCE INNOVATION BOARD.

Section 7506(g) of the Intelligence Authorization Act for Fiscal Year 2024 (Public Law 118–31) is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by inserting "active and" before "potential";

(B) in subparagraph (B), by striking "the Inspector General of the Intelligence Community" and inserting "the designated agency ethics official";

(C) by redesignating subparagraph (C) as subparagraph (D); and

(D) by inserting after subparagraph (B) the following:

"(C) Authority for the designated agency ethics official to grant a waiver for a conflict of interest, except that—

"(i) no waiver may be granted for an active conflict of interest identified with respect to the Chair of the Board;

"(ii) every waiver for a potential conflict of interest requires review and approval by the Director of National Intelligence; and

"(iii) for every waiver granted, the designated agency ethics official shall submit to the congressional intelligence committees notice of the waiver."; and

(2) by adding at the end the following:

"(3) DEFINITION OF DESIGNATED AGENCY ETHICS OFFICIAL.—In this subsection, the term 'designated agency ethics official' means the designated agency ethics official (as defined

in section 13101 of title 5, United States Code) in the Office of the Director of National Intelligence.".

SEC. 302. NATIONAL THREAT IDENTIFICATION AND PRIORITIZATION ASSESSMENT AND NATIONAL COUNTERINTELLIGENCE STRATEGY.

Section 904(f)(3) of the Counterintelligence Enhancement Act of 2002 (50 U.S.C. 3383(f)(3)) is amended by striking "National Counterintelligence Executive" and inserting "Director of the National Counterintelligence and Security Center".

SEC. 303. OPEN SOURCE INTELLIGENCE DIVISION OF OFFICE OF INTELLIGENCE AND ANALYSIS PERSONNEL.

None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2025 for the Office of Intelligence and Analysis of the Department of Homeland Security may be obligated or expended by the Office to increase, above the staffing level in effect on the day before the date of the enactment of this Act, the number of personnel assigned to the Open Source Intelligence Division who work exclusively or predominantly on domestic terrorism issues.

SEC. 304. APPOINTMENT OF DIRECTOR OF THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE.

(a) In General.—Section 215(c) of the Department of Energy Organization Act (42 U.S.C. 7144b(c)) is amended to read as follows:

"(c) Director.—

"(1) APPOINTMENT.—The head of the Office shall be the Director of the Office of Intelligence and Counterintelligence, who shall be appointed by the President, by and with the advice and consent of the Senate. The Director of the Office shall report directly to the Secretary.

"(2) TERM.—

"(A) IN GENERAL.—The Director shall serve for a term of 6 years.

"(B) REAPPOINTMENT.—The Director shall be eligible for reappointment for 1 or more terms.

"(3) QUALIFICATIONS.—The Director shall—

"(A) be an employee in the Senior Executive Service, the Senior Intelligence Service, the Senior National Intelligence Service, or any other Service that the Secretary, in coordination with the Director of National Intelligence, considers appropriate; and

"(B) have substantial expertise in matters relating to the intelligence community,

including foreign intelligence and counterintelligence.”.

(b) Effective Date.—The amendment made by this section shall take effect on January 21, 2025.

SEC. 305. IMPROVEMENTS TO ADVISORY BOARD OF NATIONAL RECONNAISSANCE OFFICE.

Section 106A(d) of the National Security Act of 1947 (50 U.S.C. 3041a(d)) is amended—

(1) in paragraph (3)(A)—

(A) in clause (i)—

(i) by striking “five members appointed by the Director, in consultation with the Director of National Intelligence and the Secretary of Defense,” and inserting “up to 8 members appointed by the Director”; and

(ii) by inserting “, and who do not present any actual or potential conflict of interest” before the period at the end;

(B) by redesignating clause (ii) as clause (iii); and

(C) by inserting after clause (i) the following:

“(ii) MEMBERSHIP STRUCTURE.—The Director shall ensure that no more than 2 concurrently serving members of the Board qualify for membership on the Board based predominantly on a single qualification set forth under clause (i).”;

(2) by redesignating paragraphs (5) through (7) as paragraphs (6) through (8), respectively;

(3) by inserting after paragraph (4) the following:

“(5) CHARTER.—The Director shall establish a charter for the Board that includes the following:

“(A) Mandatory processes for identifying potential conflicts of interest, including the submission of initial and periodic financial disclosures by Board members.

“(B) The vetting of potential conflicts of interest by the designated agency ethics official, except that no individual waiver may be granted for a conflict of interest identified with respect to the Chair of the Board.

“(C) The establishment of a process and associated protections for any whistleblower alleging a violation of applicable conflict of interest law, Federal contracting law, or other provision of law.”; and

(4) in paragraph (8), as redesignated by paragraph (2), by striking “September 30, 2024” and inserting “August 31, 2027”.

SEC. 306. NATIONAL INTELLIGENCE UNIVERSITY ACCEPTANCE OF GRANTS.

(a) In General.—Subtitle D of title X of the National Security Act of 1947 (50 U.S.C. 3227 et

seq.) is amended by adding at the end the following:

"1035. National Intelligence University acceptance of grants

"(a) Authority.—The Director of National Intelligence may authorize the President of the National Intelligence University to accept qualifying research grants.

"(b) Qualifying Grants.—A qualifying research grant under this section is a grant that is awarded on a competitive basis by an entity referred to in subsection (c) for a research project with a scientific, literary, or educational purpose.

"(c) Entities From Which Grants May Be Accepted.—A qualifying research grant may be accepted under this section only from a Federal agency or from a corporation, fund, foundation, educational institution, or similar entity that is organized and operated primarily for scientific, literary, or educational purposes.

"(d) Administration of Grant Funds.—

"(1) ESTABLISHMENT OF ACCOUNT.—The Director shall establish an account for administering funds received as qualifying research grants under this section.

"(2) USE OF FUNDS.—The President of the University shall use the funds in the account established pursuant to paragraph (1) in accordance with applicable provisions of the regulations and the terms and conditions of the grants received.

"(e) Related Expenses.—Subject to such limitations as may be provided in appropriations Acts, appropriations available for the National Intelligence University may be used to pay expenses incurred by the University in applying for, and otherwise pursuing, the award of qualifying research grants.

"(f) Regulations.—The Director of National Intelligence shall prescribe regulations for the administration of this section.".

(b) Clerical Amendment.—The table of contents preceding section 2 of such Act is amended by inserting after the item relating to section 1034 the following new item:

"Sec.1035.National Intelligence University acceptance of grants.".

SEC. 307. PROTECTION OF CENTRAL INTELLIGENCE AGENCY FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

The Central Intelligence Agency Act of 1949 (50 U.S.C. 3501 et seq.) is amended by inserting after section 15 the following new section (and conforming the table of contents at the beginning of such Act accordingly):

"SEC. 15A. PROTECTION OF CERTAIN FACILITIES AND ASSETS FROM UNMANNED AIRCRAFT.

"(a) Definitions.—In this section:

"(1) BUDGET.—The term 'budget', with respect to a fiscal year, means the budget for that

fiscal year that is submitted to Congress by the President under section 1105(a) of title 31, United States Code.

"(2) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term 'congressional intelligence committees' means—

"(A) the Select Committee on Intelligence of the Senate;

"(B) the Permanent Select Committee on Intelligence of the House of Representatives;

"(C) the Subcommittee on Defense of the Committee on Appropriations of the Senate; and

"(D) the Subcommittee on Defense of the Committee on Appropriations of the House of Representatives.

"(3) CONGRESSIONAL JUDICIARY COMMITTEES.—The term 'congressional judiciary committees' means—

"(A) the Committee on the Judiciary of the Senate; and

"(B) the Committee on the Judiciary of the House of Representatives.

"(4) CONGRESSIONAL TRANSPORTATION AND INFRASTRUCTURE COMMITTEES.—The term 'congressional transportation and infrastructure committees' means—

"(A) the Committee on Commerce, Science, and Transportation of the Senate; and

"(B) the Committee on Transportation and Infrastructure of the House of Representatives.

"(5) COVERED FACILITY OR ASSET.—The term 'covered facility or asset' means property owned, leased, or controlled by the Agency, property controlled and occupied by the Federal Highway Administration, located immediately adjacent to the headquarters compound of the Agency, and property owned, leased, or controlled by the Office of the Director of National Intelligence where the property—

"(A) is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Director, in coordination with the Secretary of Transportation, with respect to potentially impacted airspace, through a risk-based assessment for purposes of this section;

"(B) is located in the United States and beneath airspace that is prohibited or restricted by the Federal Aviation Administration;

"(C) is a property of which Congress has been notified is covered under this paragraph; and

"(D) directly relates to one or more functions authorized to be performed by the Agency, pursuant to the National Security Act of 1947 (50 U.S.C. 3001) or this Act.

"(6) ELECTRONIC COMMUNICATION.—The term 'electronic communication' has the meaning given such term in section 2510 of title 18, United States Code.

"(7) INTERCEPT.—The term 'intercept' has the meaning given such term in section 2510

of title 18, United States Code.

"(8) ORAL COMMUNICATION.—The term 'oral communication' has the meaning given such term in section 2510 of title 18, United States Code.

"(9) RADIO COMMUNICATION.—The term 'radio communication' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

"(10) RISK-BASED ASSESSMENT.—The term 'risk-based assessment' includes an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the National Airspace System and the needs of national security at each covered facility or asset identified by the Director, an evaluation of each of the following factors:

"(A) Potential impacts to safety, efficiency, and use of the National Airspace System, including potential effects on manned aircraft and unmanned aircraft systems, aviation safety, airport operations, infrastructure, and air navigation services relating to the use of any system or technology for carrying out the actions described in subsection (c)(1).

"(B) Options for mitigating any identified impacts to the National Airspace System relating to the use of any system or technology, including minimizing when possible the use of any system or technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

"(C) Potential consequences of the effects of any actions taken under subsection (c)(1) to the National Airspace System and infrastructure if not mitigated.

"(D) The ability to provide reasonable advance notice to aircraft operators consistent with the safety of the National Airspace System and the needs of national security.

"(E) The setting and character of any covered facility or asset, including whether it is located in a populated area or near other structures, and any potential for interference with wireless communications or for injury or damage to persons or property.

"(F) Potential consequences to national security if threats posed by unmanned aircraft systems or unmanned aircraft are not mitigated or defeated.

"(11) UNITED STATES.—The term 'United States' has the meaning given that term in section 5 of title 18, United States Code.

"(12) UNMANNED AIRCRAFT; UNMANNED AIRCRAFT SYSTEM.—The terms 'unmanned aircraft' and 'unmanned aircraft system' have the meanings given those terms in section 44801 of title 49, United States Code.

"(13) WIRE COMMUNICATION.—The term 'wire communication' has the meaning given such term in section 2510 of title 18, United States Code.

"(b) Authority.—Notwithstanding section 46502 of title 49, United States Code, or sections 32, 1030, and 1367 and chapters 119 and 206 of title 18, United States Code, or section 705 of the Communications Act of 1934 (47 U.S.C. 605), the Director may take, and may authorize Agency personnel with assigned duties that include the security or protection of people, facilities, or assets within the United States to take—

"(1) such actions described in subsection (c)(1) that are necessary to mitigate a credible threat (as defined by the Director, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset; and

"(2) such actions described in subsection (c)(3).

"(c) Actions.—

"(1) ACTIONS DESCRIBED.—The actions described in this paragraph are the following:

"(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.

"(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active and by direct or indirect physical, electronic, radio, or electromagnetic means.

"(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

"(D) Seize or exercise control over the unmanned aircraft system or unmanned aircraft.

"(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

"(F) Use reasonable force, if necessary, to seize or otherwise disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

"(2) COORDINATION.—The Director shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

"(3) RESEARCH, TESTING, TRAINING, AND EVALUATION.—

"(A) IN GENERAL.—The Director shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine the capability and utility of the equipment prior to the use of the equipment for any action described in paragraph (1).

"(B) PERSONNEL.—Personnel and contractors who do not have assigned duties that include the security or protection of people, facilities, or assets may engage in research, testing, training, and evaluation activities pursuant to subparagraph (A).

"(4) FAA COORDINATION.—The Director shall coordinate with the Administrator of the Federal Aviation Administration on any action described in paragraph (1) or (3) so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely affect or interfere with safe airport operations, navigation, air traffic

services, or the safe and efficient operation of the National Airspace System.

"(d) Forfeiture.—Any unmanned aircraft system or unmanned aircraft that is seized pursuant to subsection (b) as described in subsection (c)(1) is subject to forfeiture to the United States.

"(e) Regulations and Guidance.—

"(1) ISSUANCE.—The Director and the Secretary of Transportation may each prescribe regulations, and shall each issue guidance, to carry out this section.

"(2) COORDINATION.—

"(A) REQUIREMENT.—The Director shall coordinate the development of guidance under paragraph (1) with the Secretary of Transportation.

"(B) AVIATION SAFETY.—The Director shall coordinate with the Secretary of Transportation and the Administrator of the Federal Aviation Administration before issuing any guidance, or otherwise implementing this section, so the Administrator may ensure that unmanned aircraft system detection and mitigation systems do not adversely affect or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the National Airspace System.

"(f) Privacy Protection.—The regulations prescribed or guidance issued under subsection (e) shall ensure that—

"(1) the interception or acquisition of, or access to, or maintenance or use of, communications to or from an unmanned aircraft system or unmanned aircraft under this section is conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States and applicable provisions of Federal law;

"(2) communications to or from an unmanned aircraft system or unmanned aircraft are intercepted or acquired only to the extent necessary to support an action described in subsection (c);

"(3) records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Director determines that maintenance of such records for a longer period is necessary for the investigation or prosecution of a violation of law, to fulfill a duty, responsibility, or function of the Agency, is required under Federal law, or for the purpose of any litigation; and

"(4) such communications are not disclosed outside the Agency unless the disclosure—

"(A) is necessary to investigate or prosecute a violation of law;

"(B) would support the Agency, the Department of Defense, a Federal law enforcement, intelligence, or security agency, a State, local, Tribal, or territorial law enforcement agency, or other relevant person or entity if such entity or person is engaged in a security or protection operation;

"(C) is necessary to support a department or agency listed in subparagraph (B) in investigating or prosecuting a violation of law;

"(D) would support the enforcement activities of a regulatory agency of the Federal Government in connection with a criminal or civil investigation of, or any regulatory,

statutory, or other enforcement action relating to, an action described in subsection (b);

"(E) is necessary to protect against dangerous or unauthorized activity by unmanned aircraft systems or unmanned aircraft;

"(F) is necessary to fulfill a duty, responsibility, or function of the Agency; or

"(G) is otherwise required by law.

"(g) Budget.—

"(1) IN GENERAL.—The Director shall submit to the congressional intelligence committees, as a part of the budget request of the Agency for each fiscal year after fiscal year 2025, a consolidated funding display that identifies the funding source for the actions described in subsection (c)(1) within the Agency.

"(2) FORM.—Each funding display submitted pursuant to paragraph (1) shall be in unclassified form, but may contain a classified annex.

"(h) Semiannual Briefings and Notifications.—

"(1) BRIEFINGS.—Not later than 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 and semiannually thereafter, the Director shall provide the congressional intelligence committees, the congressional judiciary committees, and the congressional transportation and infrastructure committees a briefing on the activities carried out pursuant to this section during the period covered by the briefing.

"(2) REQUIREMENT.—Each briefing under paragraph (1) shall be conducted jointly with the Secretary of Transportation.

"(3) CONTENTS.—Each briefing under paragraph (1) shall include, for the period covered by the briefing, the following:

"(A) Policies, programs, and procedures to mitigate or eliminate the effects of the activities described in paragraph (1) to the National Airspace System and other critical national transportation infrastructure.

"(B) A description of instances in which actions described in subsection (c)(1) have been taken, including all such instances that may have resulted in harm, damage, or loss to a person or to private property.

"(C) A description of the guidance, policies, or procedures established to address privacy, civil rights, and civil liberties issues affected by the actions allowed under this section, as well as any changes or subsequent efforts that would significantly affect privacy, civil rights, or civil liberties.

"(D) A description of options considered and steps taken to mitigate any identified effects on the National Airspace System relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

"(E) A description of instances in which communications intercepted or acquired

during the course of operations of an unmanned aircraft system or unmanned aircraft were maintained for more than 180 days or disclosed outside the Agency.

"(F) How the Director and the Secretary of Transportation have informed the public as to the possible use of authorities under this section.

"(G) How the Director and the Secretary of Transportation have engaged with Federal, State, local, territorial, or Tribal law enforcement agencies to implement and use such authorities.

"(H) An assessment of whether any gaps or insufficiencies remain in statutes, regulations, and policies that impede the ability of the Agency to counter the threat posed by the malicious use of unmanned aircraft systems and unmanned aircraft and any recommendations to remedy such gaps or insufficiencies.

"(4) FORM.—Each briefing under paragraph (1) shall be in unclassified form, but may be accompanied by an additional classified report.

"(5) NOTIFICATION.—

"(A) IN GENERAL.—Within 30 days of deploying any new technology to carry out the actions described in subsection (c)(1), the Director shall submit to the congressional intelligence committees a notification of the deployment of such technology.

"(B) CONTENTS.—Each notification submitted pursuant to subparagraph (A) shall include a description of options considered to mitigate any identified effects on the National Airspace System relating to the use of any system or technology, including the minimization of the use of any technology that disrupts the transmission of radio or electronic signals, for carrying out the actions described in subsection (c)(1).

"(i) Rule of Construction.—Nothing in this section may be construed—

"(1) to vest in the Director any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration; or

"(2) to vest in the Secretary of Transportation or the Administrator of the Federal Aviation Administration any authority of the Director.

"(j) Termination.—

"(1) IN GENERAL.—Except as provided in paragraph (2), the authority to carry out this section with respect to the actions specified in subparagraphs (B) through (F) of subsection (c)(1), shall terminate on the date that is 4 years after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025.

"(2) EXTENSION.—The President may extend by 1 year the termination date specified in paragraph (1) if, before termination, the President certifies to Congress that such extension is in the national security interests of the United States.

"(k) Scope of Authority.—Nothing in this section shall be construed to provide the Director or the Secretary of Transportation with additional authorities beyond those described in subsections (b) and (d).".

SEC. 308. LIMITATION ON AVAILABILITY OF FUNDS FOR NEW CONTROLLED ACCESS PROGRAMS.

None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2025 for the National Intelligence Program may be obligated or expended for any controlled access program (as defined in section 501A(d) of the National Security Act of 1947 (50 U.S.C. 3091a(d))), or a compartment or subcompartment therein, that is established on or after the date of the enactment of this Act, until the head of the element of the intelligence community responsible for the establishment of such program, compartment, or subcompartment, submits the notification required by section 501A(b) of the National Security Act of 1947 (50 U.S.C. 3091a(b)).

SEC. 309. LIMITATION ON TRANSFERS FROM CONTROLLED ACCESS PROGRAMS.

Section 501A(b) of the National Security Act of 1947 (50 U.S.C. 3091a(b)) is amended—

(1) in the subsection heading, by striking "Limitation on Establishment" and inserting "Limitations";

(2) by striking "A head" and inserting the following:

"(1) ESTABLISHMENT.—A head"; and

(3) by adding at the end the following:

"(2) TRANSFERS.—A head of an element of the intelligence community may not transfer a capability from a controlled access program, including from a compartment or subcompartment therein to a compartment or subcompartment of another controlled access program, to a special access program (as defined in section 1152(g) of the National Defense Authorization Act for Fiscal Year 1994 (50 U.S.C. 3348(g))), or to anything else outside the controlled access program, until the head submits to the appropriate congressional committees and congressional leadership notice of the intent of the head to make such transfer.".

SEC. 310. EXPENDITURE OF FUNDS FOR CERTAIN INTELLIGENCE AND COUNTERINTELLIGENCE ACTIVITIES OF THE COAST GUARD.

The Commandant of the Coast Guard may use up to 1 percent of the amounts made available for the National Intelligence Program (as such term is defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) for each fiscal year for intelligence and counterintelligence activities of the Coast Guard relating to objects of a confidential, extraordinary, or emergency nature, which amounts may be accounted for solely on the certification of the Commandant and each such certification shall be considered to be a sufficient voucher for the amount contained in the certification.

SEC. 311. UNAUTHORIZED ACCESS TO INTELLIGENCE

COMMUNITY PROPERTY.

(a) In General.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended by adding at the end the following:

"SEC. 1115. UNAUTHORIZED ACCESS TO INTELLIGENCE COMMUNITY PROPERTY.

"(a) In General.—It shall be unlawful, within the jurisdiction of the United States, without authorization to access any property that—

"(1) is under the jurisdiction of an element of the intelligence community; and

"(2) has been clearly marked as closed or restricted.

"(b) Penalties.—Any person who violates subsection (a) shall—

"(1) in the case of the first offense, be fined under title 18, United States Code, imprisoned for not more than 180 days, or both;

"(2) in the case of the second offense, be fined under such title, imprisoned for not more than 3 years, or both; and

"(3) in the case of the third or subsequent offense, be fined under such title, imprisoned for not more than 10 years, or both.".

(b) Clerical Amendment.—The table of contents preceding section 2 of such Act is amended by adding at the end the following:

"Sec.1115.Unauthorized access to intelligence community property.".

SEC. 312. STRENGTHENING OF OFFICE OF INTELLIGENCE AND ANALYSIS.

(a) In General.—Section 311 of title 31, United States Code, is amended to read as follows:

"311. Office of Economic Intelligence and Security

"(a) Definitions.—In this section, the terms 'counterintelligence', 'foreign intelligence', and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

"(b) Establishment.—There is established within the Office of Terrorism and Financial Intelligence of the Department of the Treasury, the Office of Economic Intelligence and Security (in this section referred to as the 'Office'), which shall—

"(1) be responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information relating to the operation and responsibilities of the Department of the Treasury and other Federal agencies executing economic statecraft tools that do not include any elements that are elements of the intelligence community;

"(2) provide intelligence support and economic analysis to Federal agencies

implementing United States economic policy, including for purposes of global strategic competition; and

"(3) have such other related duties and authorities as may be assigned by the Secretary for purposes of the responsibilities described in paragraph (1), subject to the authority, direction, and control of the Secretary, in consultation with the Director of National Intelligence.

"(c) Assistant Secretary for Economic Intelligence and Security.—The Office shall be headed by an Assistant Secretary, who shall be appointed by the President, by and with the advice and consent of the Senate. The Assistant Secretary shall report directly to the Undersecretary for Terrorism and Financial Crimes.".

(b) Clerical Amendment.—The table of sections at the beginning of chapter 3 of such title is amended by striking the item relating to section 311 and inserting the following:

"311. Office of Economic Intelligence and Security.".

(c) Conforming Amendment.—Section 3(4)(J) of the National Security Act of 1947 (50 U.S.C. 3003(4)(J)) is amended by striking "Office of Intelligence and Analysis" and inserting "Office of Economic Intelligence and Security".

(d) References.—Any reference in a law, regulation, document, paper, or other record of the United States to the Office of Intelligence and Analysis of the Department of the Treasury shall be deemed a reference to the Office of Economic Intelligence and Security of the Department of the Treasury.

SEC. 313. REPORT ON SENSITIVE COMMERCIALLY AVAILABLE INFORMATION.

(a) Definitions.—

(1) COMMERCIALLY AVAILABLE INFORMATION.—The term "commercially available information" means—

(A) any data or other information of the type customarily made available or obtainable and sold, leased, or licensed to members of the general public or to non-governmental entities for purposes other than governmental purposes; or

(B) data and information for exclusive government use knowingly and voluntarily provided by, procured from, or made accessible by corporate entities on their own initiative or at the request of a government entity.

(2) PERSONALLY IDENTIFIABLE INFORMATION.—The term "personally identifiable information" means information that, alone or when combined with other information regarding an individual, can be used to distinguish or trace the identity of such individual.

(3) SENSITIVE ACTIVITIES.—The term "sensitive activities" means activities that, over an extended period of time—

(A) establish a pattern of life;

(B) reveal personal affiliations, preferences, or identifiers;

(C) facilitate prediction of future acts;

(D) enable targeting activities;

(E) reveal the exercise of individual rights and freedoms, including the rights to freedom of speech and of the press, to free exercise of religion, to peaceably assemble, including membership or participation in organizations or associations, and to petition the government; or

(F) reveal any other activity the disclosure of which could cause substantial harm, embarrassment, inconvenience, or unfairness to the United States person who engaged in the activity.

(4) SENSITIVE COMMERCIALLY AVAILABLE INFORMATION.—The term "sensitive commercially available information"—

(A) means commercially available information that is known or reasonably expected to contain—

(i) a substantial volume of personally identifiable information regarding United States persons; or

(ii) a greater than de minims volume of sensitive data;

(B) shall not include—

(i) newspapers or other periodicals;

(ii) weather reports;

(iii) books;

(iv) journal articles or other published works;

(v) public filings or records;

(vi) documents or databases similar to those described in clauses (i) through (v), whether accessed through a subscription or accessible free of cost; or

(vii) limited data samples made available to elements of the intelligence community for the purposes of allowing such elements to determine whether to purchase the full dataset and not accessed, retained, or used for any other purpose.

(5) SENSITIVE DATA.—The term "sensitive data" means data that—

(A)(i) captures personal attributes, conditions, or identifiers that are traceable to 1 or more specific United States persons, either through the dataset or by correlating the dataset with other available information; and

(ii) concerns the race or ethnicity, political opinions, religious beliefs, sexual orientation, gender identity, medical or genetic information, financial data, or any other data with respect to such specific United States person or United States persons the disclosure of which would have the potential to cause substantial harm, embarrassment, inconvenience, or unfairness to the United States person or United States persons described by the data; or

(B) captures the sensitive activities of 1 or more United States persons.

(6) UNITED STATES PERSON.—The term "United States person" means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an unorganized association substantially composed of United States citizens or permanent resident aliens; or

(C) an entity organized under the laws of the United States or of any jurisdiction within the United States, with the exception of any such entity directed or controlled by a foreign government.

(b) Report.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and annually thereafter, the head of each element of the intelligence community shall submit to the congressional intelligence committees a report on the access to, collection, processing, and use of sensitive commercially available information by the respective element.

(2) CONTENTS.—

(A) IN GENERAL.—For each dataset containing sensitive commercially available information accessed, collected, processed, or used by the element concerned for purposes other than research and development, a report required by paragraph (1) shall include the following:

(i) A description of the nature and volume of the sensitive commercially available information accessed or collected by the element.

(ii) A description of the mission or administrative need or function for which the sensitive commercially available information is accessed or collected, and of the nature, scope, reliability, and timeliness of the dataset required to fulfill such mission or administrative need or function.

(iii) A description of the purpose of the access, collection, or processing, and the intended use of the sensitive commercially available information.

(iv) An identification of the legal authority for the collection or access, and processing of the sensitive commercially available information.

(v) An identification of the source of the sensitive commercially available information and the persons from whom the sensitive commercially available information was accessed or collected.

(vi) A description of the mechanics of the access, collection, and processing of the sensitive commercially available information, including the Federal entities that participated in the procurement process.

(vii) A description of the method by which the element has limited the access to and collection and processing of the sensitive commercially available information to the maximum extent feasible consistent with the need to fulfill the mission or administrative need.

(viii) An assessment of whether the mission or administrative need can be

fulfilled if reasonably available privacy-enhancing techniques, such as filtering or anonymizing, the application of traditional safeguards, including access limitations and retention limits, differential privacy techniques, or other information-masking techniques, such as restrictions or correlation, are implemented with respect to information concerning United States persons.

(ix) An assessment of the privacy and civil liberties risks associated with accessing, collecting, or processing the data and the methods by which the element mitigates such risks.

(x) An assessment of the applicability of section 552a of title 5, United States Code (commonly referred to as the "Privacy Act of 1974"), if any.

(xi) To the extent feasible, an assessment of the original source of the data and the method through which the dataset was generated and aggregated, and whether any element of the intelligence community previously accessed or collected the same or similar sensitive commercially available information from the source.

(xii) An assessment of the quality and integrity of the data, including, as appropriate, whether the sensitive commercially available information reflects any underlying biases or inferences, and efforts to ensure that any intelligence products created with the data are consistent with the standards of the intelligence community for accuracy and objectivity.

(xiii) An assessment of the security, operational, and counterintelligence risks associated with the means of accessing or collecting the data, and recommendations for how the element could mitigate such risks.

(xiv) A description of the system in which the data is retained and processed and how the system is properly secured while allowing for effective implementation, management, and audit, as practicable, of relevant privacy and civil liberties protections.

(xv) An assessment of security risks posed by the system architecture of vendors providing sensitive commercially available information or access to such sensitive commercially available information, access restrictions for the data repository of each such vendor, and the vendor's access to query terms and, if any, relevant safeguards.

(xvi) A description of procedures to restrict access to the sensitive commercially available information.

(xvii) A description of procedures for conducting, approving, documenting, and auditing queries, searches, or correlations with respect to the sensitive commercially available information.

(xviii) A description of procedures for restricting dissemination of the sensitive commercially available information, including deletion of information of United States persons returned in response to a query or other search unless the information is assessed to be associated or potentially associated with the documented mission-related justification for the query or search.

(xix) A description of masking and other privacy-enhancing techniques used by the element to protect sensitive commercially available information.

(xx) A description of any retention and deletion policies.

(xxi) A determination of whether unevaluated data or information has been made available to other elements of the intelligence community or foreign partners and, if so, identification of those elements or partners.

(xxii) A description of any licensing agreements or contract restrictions with respect to the sensitive commercially available information.

(xxiii) A data management plan for the lifecycle of the data, from access or collection to disposition.

(xxiv) For any item required by clauses (i) through (xxiii) that cannot be completed due to exigent circumstances relating to collecting, accessing, processing, or using sensitive commercially available information, a description of such exigent circumstances.

(B) RESEARCH AND DEVELOPMENT DATA.—For each dataset containing sensitive commercially available information accessed, collected, processed, or used by the element concerned solely for research and development purposes, a report required by paragraph (1) may be limited to a description of the oversight by the element of such access, collection, process, and use.

(c) Public Report.—The Director of National Intelligence shall make available to the public, once every 2 years, a report on the policies and procedures of the intelligence community with respect to access to and collection, processing, and safeguarding of sensitive commercially available information.

SEC. 314. POLICY ON COLLECTION OF UNITED STATES LOCATION INFORMATION.

(a) Definitions.—In this section:

(1) UNITED STATES LOCATION INFORMATION.—The term "United States location information" means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, user, or device in the United States, or, if the customer, subscriber, or user is known to be a United States person, outside the United States.

(2) UNITED STATES PERSON.—The term "United States person" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) In General.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the Attorney General, shall issue a policy on the collection of United States location information by the intelligence community.

(c) Content.—The policy required by subsection (a) shall address the filtering, segregation, use, dissemination, masking, and retention of United States location information.

(d) Form; Public Availability.—The policy required by subsection (a)—

(1) shall be issued in unclassified form and made available to the public; and

(2) may include a classified annex, which the Director of National Intelligence shall submit to the congressional intelligence committees.

SEC. 315. DISPLAY OF FLAGS, SEALS, AND EMBLEMS OTHER THAN THE UNITED STATES FLAG.

(a) Definitions.—In this section:

(1) EXECUTIVE AGENCY.—The term "Executive agency" has the meaning given such term in section 105 of title 5, United States Code.

(2) NATIONAL INTELLIGENCE PROGRAM.—The term "National Intelligence Program" has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(b) In General.—Any flag, seal, or emblem that is not the United States flag and is flown, draped, projected, or otherwise displayed as a visual and symbolic representation at a property, office, or other official location of an element of the intelligence community—

(1) shall be smaller than the official United States flag; and

(2) if flown, may not be displayed higher than or above the United States flag.

(c) Limitation on Availability of Funds for Displaying and Flying Flags.—None of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2025 for the National Intelligence Program, may be obligated or expended to fly or display a flag over a facility of an element of the intelligence community other than the following:

(1) The United States flag.

(2) The POW/MIA flag.

(3) The Hostage and Wrongful Detainee flag, pursuant to section 904 of title 36, United States Code.

(4) The flag of a State, insular area, or the District of Columbia at a domestic location.

(5) The flag of an Indian Tribal Government.

(6) The official branded flag of an Executive agency.

(7) The flag of an element, flag officer, or general officer of the Armed Forces.

TITLE IV—COUNTERING FOREIGN THREATS

Subtitle A—People's Republic of China

SEC. 401. STRATEGY AND OUTREACH ON RISKS POSED BY PEOPLE'S REPUBLIC OF CHINA SMARTPORT TECHNOLOGY.

(a) Strategy and Outreach Required.—The Director of the National Counterintelligence and Security Center shall develop a strategy and conduct outreach to United States industry, including shipping companies, port operators, and logistics firms, on the risks of smartport technology of the People's Republic of China and other related risks posed by entities of the People's Republic of China, including LOGINK, China Ocean Shipping Company, Limited (COSCO), China Communications Construction Company, Limited (CCCC), China Media Group (CMG), and Shanghai Zhenhua Heavy Industries Company Limited (ZPMC), to the national security of the United States, the security of United States supply chains, and commercial activity, including with respect to delays, interruption, and lockout of access to systems and technologies that enable the free flow of commerce.

(b) Consistency With Statutes and Executive Orders.—The Director shall carry out subsection (a) in a manner that is consistent with the following:

(1) Part 6 of title 33, Code of Federal Regulations, as amended by Executive Order 14116 (89 Fed. Reg. 13971; relating to amending regulations relating to the safeguarding of vessels, harbors, ports, and waterfront facilities of the United States.

(2) Executive Order 14017 (86 Fed. Reg. 11849; relating to America's supply chains), or successor order.

(3) Section 825 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31).

(c) Coordination.—The Director shall carry out subsection (a) in coordination with the Commandant of the Coast Guard, the Director of the Federal Bureau of Investigation, the Commander of the Office of Naval Intelligence, and such other heads of Federal agencies as the Director considers appropriate.

SEC. 402. ASSESSMENT OF CURRENT STATUS OF BIOTECHNOLOGY OF PEOPLE'S REPUBLIC OF CHINA.

(a) Assessment.—Not later than 30 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the National Counterproliferation and Biosecurity Center and such heads of elements of the intelligence community as the Director of National Intelligence considers appropriate, conduct an assessment of the current status of the biotechnology of the People's Republic of China, which shall include an assessment of how the People's Republic of China is supporting the biotechnology sector through both licit and illicit means, such as foreign direct investment, subsidies, talent recruitment, or other efforts.

(b) Report.—

(1) IN GENERAL.—Not later than 30 days after the date on which the Direct of National Intelligence completes the assessment required by subsection (a), the Director shall submit to the congressional intelligence committees a report on the findings of the Director with respect to the assessment.

(2) FORM.—The report submitted pursuant to paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

SEC. 403. INTELLIGENCE SHARING WITH LAW ENFORCEMENT AGENCIES ON SYNTHETIC OPIOID PRECURSOR CHEMICALS ORIGINATING IN PEOPLE'S REPUBLIC OF CHINA.

(a) Strategy Required.—The Director of National Intelligence shall, in consultation with the head of the Office of National Security Intelligence of the Drug Enforcement Administration, the Under Secretary of Homeland Security for Intelligence and Analysis, and the heads of such other agencies as the Director considers appropriate, develop a strategy to ensure robust intelligence sharing relating to the illicit trafficking of synthetic opioid precursor chemicals from the People's Republic of China and other source countries.

(b) Mechanism for Collaboration.—The Director shall develop a mechanism so that subject matter experts in elements of the Federal Government other than elements in the intelligence community, including those without security clearances, can share information with the intelligence community relating to illicit trafficking described in subsection (a).

SEC. 404. REPORT ON EFFORTS OF THE PEOPLE'S REPUBLIC OF CHINA TO EVADE UNITED STATES TRANSPARENCY AND NATIONAL SECURITY REGULATIONS.

(a) Report Required.—The Director of National Intelligence shall submit to the congressional intelligence committees a report on efforts of the People's Republic of China to evade the following:

(1) Identification under section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 10 U.S.C. 113 note).

(2) Restrictions or limitations imposed by any of the following:

(A) Section 805 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118–31).

(B) Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 41 U.S.C. 3901 note prec.).

(C) The list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury (commonly known as the "SDN list").

(D) The Entity List maintained by the Bureau of Industry and Security of the Department of Commerce and set forth in Supplement No. 4 to part 744 of title 15, Code of Federal Regulations.

(E) Commercial or dual-use export controls under the Export Control Reform Act of 2018 (50 U.S.C. 4801 et seq.) and the Export Administration Regulations.

(F) Executive Order 14105 (88 Fed. Reg. 54867; relating to addressing United States

investments in certain national security technologies and products in countries of concern), or successor order.

(G) Import restrictions on products made with forced labor implemented by U.S. Customs and Border Protection pursuant to Public Law 117–78 (22 U.S.C. 6901 note).

(b) Form.—The report submitted pursuant to subsection (a) shall be submitted in unclassified form.

SEC. 405. PLAN FOR RECRUITMENT OF MANDARIN SPEAKERS.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the appropriate congressional committees a comprehensive plan to prioritize the recruitment and training of individuals who speak Mandarin Chinese for each element of the intelligence community.

(b) Appropriate Congressional Committees.—In this section, the term "appropriate congressional committees" means—

(1) the Select Committee on Intelligence and the Committee on the Judiciary of the Senate; and

(2) the Permanent Select Committee on Intelligence and the Committee on the Judiciary of the House of Representatives.

Subtitle B—The Russian Federation

SEC. 411. ASSESSMENT OF RUSSIAN FEDERATION SPONSORSHIP OF ACTS OF INTERNATIONAL TERRORISM.

(a) Definitions.—In this section—

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Select Committee on Intelligence, the Committee on Foreign Relations, and the Committee on Armed Services of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, and the Committee on Armed Services of the House of Representatives.

(2) FOREIGN TERRORIST ORGANIZATION.—The term "foreign terrorist organization" means an organization that has been designated as a foreign terrorist organization by the Secretary of State, pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(3) SPECIALLY DESIGNATED GLOBAL TERRORIST ORGANIZATION.—The term "specially designated global terrorist organization" means an organization that has been designated as a specially designated global terrorist by the Secretary of State or the Secretary, pursuant to

Executive Order 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).

(4) STATE SPONSOR OF TERRORISM.—The term "state sponsor of terrorism" means a country the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism, for purposes of—

(A) section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(c)(1)(A)(i));

(B) section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371);

(C) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or

(D) any other provision of law.

(b) Assessment Required.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall conduct and submit to the appropriate congressional committees an assessment on the extent to which the Russian Federation—

(1) provides support for acts of international terrorism; and

(2) cooperates with the antiterrorism efforts of the United States.

(c) Elements.—The assessment required by subsection (b) shall include the following:

(1) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has failed to show support for or cooperate with the United States on international efforts to combat terrorism, such as apprehending, prosecuting, or extraditing suspected and known terrorists, including members of foreign terrorist organizations, and sharing intelligence to deter terrorist attacks.

(2) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has provided financial, material, technical, or lethal support to foreign terrorist organizations, specially designated global terrorist organizations, state sponsors of terrorism, or for acts of international terrorism.

(3) A list of all instances in which the Russian Federation, or an official of the Russian Federation, has willfully aided or abetted—

(A) the international proliferation of nuclear explosive devices to persons;

(B) a person in acquiring unsafeguarded special nuclear material; or

(C) the efforts of a person to use, develop, produce, stockpile, or otherwise acquire chemical, biological, or radiological weapons.

(4) A determination of whether the activities of the Wagner Group constitute acts of international terrorism and whether such activities continue under any of the successor entities of the Wagner Group, including Afrika Corps.

(d) Form.—The assessment required by subsection (b) shall be submitted in unclassified form, but may include a classified annex.

(e) Briefings.—Not later than 30 days after submission of the assessment required by subsection (b), the Director of National Intelligence shall provide a classified briefing to the

appropriate congressional committees on the methodology and findings of the assessment.

SEC. 412. ASSESSMENT OF LIKELY COURSE OF WAR IN UKRAINE.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in collaboration with the Director of the Defense Intelligence Agency and the Director of the Central Intelligence Agency, shall submit to the congressional intelligence committees an assessment of the likely course of the war in Ukraine through December 31, 2025.

(b) Elements.—The assessment required by subsection (a) shall include an assessment of each of the following:

(1) The ability of the military of Ukraine to defend against Russian aggression if the United States does, or does not, continue to provide military and economic assistance to Ukraine during the period described in such subsection.

(2) The likely course of the war during such period if the United States does, or does not, continue to provide military and economic assistance to Ukraine.

(3) The ability and willingness of countries in Europe and outside of Europe to continue to provide military and economic assistance to Ukraine if the United States does, or does not, do so, including the ability of such countries to make up for any shortfall in United States assistance.

(4) The effects of a potential defeat of Ukraine by the Russian Federation on the potential for further aggression from the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, and the Democratic People's Republic of Korea.

(c) Form.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

Subtitle C—International Terrorism

SEC. 421. INCLUSION OF HAMAS, HEZBOLLAH, AL-QAEDA, AND ISIS OFFICIALS AND MEMBERS AMONG ALIENS ENGAGED IN TERRORIST ACTIVITY.

Section 212(a)(3)(B)(i) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)) is amended, in the undesignated matter following subparagraph (IX), by striking "or spokesman of the Palestine Liberation Organization" and inserting "spokesperson, or member of the Palestine Liberation Organization, Hamas, Hezbollah, Al-Qaeda, ISIS, or any successor or affiliate group, or who endorses or espouses terrorist activities conducted by any of the aforementioned groups,".

SEC. 422. ASSESSMENT AND REPORT ON THE THREAT OF ISIS-KHORASAN TO THE UNITED STATES.

(a) In General.—Not later than 60 days after the date of the enactment of this Act, the Director of the National Counterterrorism Center, in coordination with such elements of the intelligence community as the Director considers relevant, shall—

(1) conduct an assessment of the threats to the United States and United States citizens posed by ISIS-Khorasan; and

(2) submit to the congressional intelligence committees a written report on the findings of the assessment.

(b) Report Elements.—The report required by subsection (a) shall include the following:

(1) A description of the historical evolution of ISIS-Khorasan, beginning with Al-Qaeda and the attacks on the United States on September 11, 2001.

(2) A description of the ideology and stated intentions of ISIS-Khorasan as related to the United States and the interests of the United States, including the homeland.

(3) A list of all terrorist attacks worldwide attributable to ISIS-Khorasan or for which ISIS-Khorasan claimed credit, beginning on January 1, 2015.

(4) A description of the involvement of ISIS-Khorasan in Afghanistan before, during, and after the withdrawal of United States military and civilian personnel and resources in August 2021.

(5) The recruiting and training strategy of ISIS-Khorasan following the withdrawal described in paragraph (4), including—

(A) the geographic regions in which ISIS-Khorasan is physically present;

(B) regions from which ISIS-Khorasan is recruiting; and

(C) its ambitions for individual actors worldwide and in the United States.

(6) A description of the relationship between ISIS-Khorasan and ISIS core, the Taliban, Al-Qaeda, and other terrorist groups, as appropriate.

(7) A description of the association of members of ISIS-Khorasan with individuals formerly detained at United States Naval Station, Guantanamo Bay, Cuba.

(8) A description of ISIS-Khorasan's development of, and relationships with, travel facilitation networks in Europe, Central Asia, Eurasia, and Latin America.

(9) An assessment of ISIS-Khorasan's understanding of the border and immigration policies and enforcement of the United States.

(10) An assessment of the known travel of members of ISIS-Khorasan within the Western Hemisphere and specifically across the southern border of the United States.

(c) Form.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 423. TERRORIST FINANCING PREVENTION.

(a) Definitions.—In this section:

(1) DIGITAL ASSET.—The term "digital asset" means any digital representation of value

24cv3373_24-02439_000312

that is recorded on a cryptographically secured distributed ledger or any similar technology, or another implementation which was designed and built as part of a system to leverage or replace blockchain or distributed ledger technology or their derivatives.

(2) DIGITAL ASSET PROTOCOL.—The term "digital asset protocol" means any communication protocol, smart contract, or other software—

(A) deployed through the use of distributed ledger or similar technology; and

(B) that provides a mechanism for users to interact and agree to the terms of a trade for digital assets.

(3) FOREIGN DIGITAL ASSET TRANSACTION FACILITATOR.—The term "foreign digital asset transaction facilitator" means any foreign person or group of foreign persons that, as determined by the Secretary, controls, operates, or makes available a digital asset protocol or similar facility, or otherwise materially assists in the purchase, sale, exchange, custody, or other transaction involving an exchange or transfer of value using digital assets.

(4) FOREIGN FINANCIAL INSTITUTION.—The term "foreign financial institution" has the meaning given that term under section 561.308 of title 31, Code of Federal Regulations.

(5) FOREIGN PERSON.—The term "foreign person" means an individual or entity that is not a United States person.

(6) FOREIGN TERRORIST ORGANIZATION.—The term "foreign terrorist organization" means an organization that has been designated as a foreign terrorist organization by the Secretary of State, pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(7) GOOD.—The term "good" means any article, natural or manmade substance, material, supply, or manufactured product, including inspection and test equipment, and excluding technical data.

(8) SECRETARY.—The term "Secretary" means the Secretary of the Treasury.

(9) SPECIALLY DESIGNATED GLOBAL TERRORIST ORGANIZATION.—The term "specially designated global terrorist organization" means an organization that has been designated as a specially designated global terrorist by the Secretary of State or the Secretary, pursuant to Executive Order 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism).

(10) UNITED STATES PERSON.—The term "United States person" means—

(A) an individual who is a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person in the United States.

(b) Sanctions With Respect to Foreign Financial Institutions and Foreign Digital Asset Transaction Facilitators That Engage in Certain Transactions.—

(1) MANDATORY IDENTIFICATION.—Not later than 60 days after the date of enactment of

this Act, and periodically thereafter, the Secretary shall identify and submit to the President a report identifying any foreign financial institution or foreign digital asset transaction facilitator that has knowingly—

(A) facilitated a significant financial transaction with—

(i) a Foreign Terrorist Organization;

(ii) a specially designated global terrorist organization; or

(iii) a person identified on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control of the Department of the Treasury, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) for acting on behalf of or at the direction of, or being owned or controlled by, a foreign terrorist organization or a specially designated global terrorist organization; or

(B) engaged in money laundering to carry out an activity described in subparagraph (A).

(2) IMPOSITION OF SANCTIONS.—

(A) FOREIGN FINANCIAL INSTITUTIONS.—The President shall prohibit, or impose strict conditions on, the opening or maintaining of a correspondent account or a payable-through account in the United States by a foreign financial institution identified under paragraph (1).

(B) FOREIGN DIGITAL ASSET TRANSACTION FACILITATORS.—The President, pursuant to such regulations as the President may prescribe, shall prohibit any transactions between any person subject to the jurisdiction of the United States and a foreign digital asset transaction facilitator identified under paragraph (1).

(3) IMPLEMENTATION AND PENALTIES.—

(A) IMPLEMENTATION.—The President may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702, 1704) to the extent necessary to carry out this Act.

(B) PENALTIES.—The penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) shall apply to a person that violates, attempts to violate, conspires to violate, or causes a violation of regulations prescribed under this section to the same extent that such penalties apply to a person that commits an unlawful act described in subsection (a) of such section 206.

(4) PROCEDURES FOR JUDICIAL REVIEW OF CLASSIFIED INFORMATION.—

(A) IN GENERAL.—If a finding under this subsection, or a prohibition, condition, or penalty imposed as a result of any such finding, is based on classified information (as defined in section 1(a) of the Classified Information Procedures Act (18 U.S.C. App.)), the Secretary may submit to a court reviewing the finding or the imposition of the prohibition, condition, or penalty such classified information ex parte and in camera.

(B) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to

confer or imply any right to judicial review of any finding under this subsection or any prohibition, condition, or penalty imposed as a result of any such finding.

(5) WAIVER FOR NATIONAL SECURITY.—The Secretary may waive the imposition of sanctions under this subsection with respect to a person if the Secretary—

(A) determines that such a waiver is in the national interests of the United States; and

(B) submits to Congress a notification of the waiver and the reasons for the waiver.

(6) EXCEPTION FOR INTELLIGENCE ACTIVITIES.—This subsection shall not apply with respect to any activity subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) or any authorized intelligence activities of the United States.

(7) EXCEPTION RELATING TO IMPORTATION OF GOODS.—The authorities and requirements under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(c) Special Measures for Modern Threats.—Section 5318A of title 31, United States Code, is amended—

(1) in subsection (a)(2)(C), by striking "subsection (b)(5)" and inserting "paragraphs (5) and (6) of subsection (b)"; and

(2) in subsection (b)—

(A) in paragraph (5), by striking "for or on behalf of a foreign banking institution"; and

(B) by adding at the end the following:

"(6) PROHIBITIONS OR CONDITIONS ON CERTAIN TRANSMITTALS OF FUNDS.—If the Secretary finds a jurisdiction outside of the United States, 1 or more financial institutions operating outside of the United States, 1 or more types of accounts within, or involving, a jurisdiction outside of the United States, or 1 or more classes of transactions within, or involving, a jurisdiction outside of the United States to be of primary money laundering concern, the Secretary, in consultation with the Secretary of State, the Attorney General, and the Chairman of the Board of Governors of the Federal Reserve System, may prohibit, or impose conditions upon, certain transmittals of funds (as such term may be defined by the Secretary in a special measure issuance, by regulation, or as otherwise permitted by law), to or from any domestic financial institution or domestic financial agency if such transmittal of funds involves any such jurisdiction, institution, type of account, class of transaction, or type of account.".

(d) Funding.—There is authorized to be appropriated to the Secretary such funds as are necessary to carry out the purposes of this section.

Subtitle D—Other Foreign Threats

SEC. 431. ASSESSMENT OF VISA-FREE TRAVEL TO AND

WITHIN WESTERN HEMISPHERE BY NATIONALS OF COUNTRIES OF CONCERN.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a written assessment of the impacts to national security caused by travel without a visa to and within countries in the Western Hemisphere by nationals of countries of concern.

(b) Form.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) Countries of Concern Defined.—In this section, the term "countries of concern" means—

(1) the Russian Federation;

(2) the People's Republic of China;

(3) the Islamic Republic of Iran;

(4) the Syrian Arab Republic;

(5) the Democratic People's Republic of Korea;

(6) the Bolivarian Republic of Venezuela; and

(7) the Republic of Cuba.

SEC. 432. STUDY ON THREAT POSED BY FOREIGN INVESTMENT IN UNITED STATES AGRICULTURAL LAND.

(a) Definitions.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

(A) the Select Committee on Intelligence, the Committee on Agriculture, Nutrition, and Forestry, the Committee on Foreign Relations, and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Agriculture, the Committee on Foreign Affairs, and the Committee on Financial Services of the House of Representatives.

(2) DIRECTOR.—The term "Director" means the Director of National Intelligence.

(3) NONMARKET ECONOMY COUNTRY.—The term "nonmarket economy country" has the meaning given that term in section 771(18) of the Tariff Act of 1930 (19 U.S.C. 1677(18)).

(b) Study and Briefing.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Director, in coordination with the elements of the intelligence community the Director considers appropriate and with the Secretary of State, the Secretary of Agriculture, and the

Secretary of the Treasury, shall—

(A) complete a study on the threat posed to the United States by foreign investment in agricultural land in the United States; and

(B) provide to the appropriate committees of Congress a briefing on the results of the study.

(2) DATA.—In conducting the study required by paragraph (1), the Director shall process and analyze relevant data collected by the Secretary of State, the Secretary of Agriculture, and the Secretary of the Treasury, including the information submitted to the Secretary of Agriculture under section 2 of the Agricultural Foreign Investment Disclosure Act of 1978 (7 U.S.C. 3501).

(3) ELEMENTS.—The study required by paragraph (1) shall include the following:

(A) Data and an analysis of agricultural land holdings, including current and previous uses of the land disaggregated by sector and industry, in each county in the United States held by a foreign person from—

(i) a country identified as a country that poses a risk to the national security of the United States in the most recent annual report on worldwide threats issued by the Director pursuant to section 108B of the National Security Act of 1947 (50 U.S.C. 3043b) (commonly known as the "Annual Threat Assessment");

(ii) a nonmarket economy country; or

(iii) any other country that the Director determines to be appropriate.

(B) An analysis of the proximity of the agricultural land holdings to critical infrastructure and military installations.

(C) An assessment of the threats posed to the national security of the United States by malign actors that use foreign investment in agricultural land in the United States.

(D) An assessment of warning indicators and methods by which to detect potential threats from the use by foreign adversaries of agricultural products for nefarious ends.

(E) An assessment of additional resources or authorities necessary to counter threats identified during the study.

SEC. 433. ASSESSMENT OF THREAT POSED BY CITIZENSHIP-BY-INVESTMENT PROGRAMS.

(a) Definitions.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

(A) the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Homeland Security, the Committee on Foreign Affairs, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(2) ASSISTANT SECRETARY.—The term "Assistant Secretary" means the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury.

(3) CITIZENSHIP-BY-INVESTMENT PROGRAM.—The term "citizenship-by-investment program" means an immigration, investment, or other program of a foreign country that, in exchange for a covered contribution, authorizes the individual making the covered contribution to acquire citizenship in such country, including temporary or permanent residence that may serve as the basis for subsequent naturalization.

(4) COVERED CONTRIBUTION.—The term "covered contribution" means—

(A) an investment in, or a monetary donation or any other form of direct or indirect capital transfer to, including through the purchase or rental of real estate—

(i) the government of a foreign country; or

(ii) any person, business, or entity in such a foreign country; and

(B) a donation to, or endowment of, any activity contributing to the public good in such a foreign country.

(5) DIRECTOR.—The term "Director" means the Director of National Intelligence.

(b) Assessment of Threat Posed by Citizenship-by-investment Programs.—

(1) ASSESSMENT.—Not later than 1 year after the date of the enactment of this Act, the Director and the Assistant Secretary, in coordination with the heads of the other elements of the intelligence community and the head of any appropriate Federal agency, shall complete an assessment of the threat posed to the United States by citizenship-by-investment programs.

(2) ELEMENTS.—The assessment required by paragraph (1) shall include the following:

(A) An identification of each citizenship-by-investment program, including an identification of the foreign country that operates each such program.

(B) With respect to each citizenship-by-investment program identified under subparagraph (A)—

(i) a description of the types of investments required under the program; and

(ii) an identification of the sectors to which an individual may make a covered contribution under the program.

(C) An assessment of the threats posed to the national security of the United States by malign actors that use citizenship-by-investment programs—

(i) to evade sanctions or taxes;

(ii) to facilitate or finance—

(I) crimes relating to national security, including terrorism, weapons trafficking or proliferation, cybercrime, drug trafficking, human trafficking,

and espionage; or

(II) any other activity that furthers the interests of a foreign adversary or undermines the integrity of the immigration laws or security of the United States; or

(iii) to undermine the United States and its interests through any other means identified by the Director and the Assistant Secretary.

(D) An identification of the foreign countries the citizenship-by-investment programs of which pose the greatest threat to the national security of the United States.

(3) REPORT AND BRIEFING.—

(A) REPORT.—

(i) IN GENERAL.—Not later than 180 days after completing the assessment required by paragraph (1), the Director and the Assistant Secretary shall jointly submit to the appropriate committees of Congress a report on the findings of the Director and the Assistant Secretary with respect to the assessment.

(ii) ELEMENTS.—The report required by clause (i) shall include the following:

(I) A detailed description of the threats posed to the national security of the United States by citizenship-by-investment programs.

(II) Recommendations for additional resources or authorities necessary to counter such threats.

(III) A description of opportunities to counter such threats.

(iii) FORM.—The report required by clause (i) shall be submitted in unclassified form but may include a classified annex, as appropriate.

(B) BRIEFING.—Not later than 90 days after the date on which the report required by subparagraph (A) is submitted, the Director and Assistant Secretary shall provide the appropriate committees of Congress with a briefing on the report.

SEC. 434. MITIGATING THE USE OF UNITED STATES COMPONENTS AND TECHNOLOGY IN HOSTILE ACTIVITIES BY FOREIGN ADVERSARIES.

(a) Findings.—Congress finds the following:

(1) Foreign defense material, including advanced military and intelligence capabilities, continues to rely heavily on products and services sourced from the United States.

(2) Iran drones operating against Ukraine were found to include several United States components.

(3) The components described in paragraph (2) came from 13 different United States companies and are integral to the operation of the drones.

(4) The Chinese spy balloon that flew across the United States in 2023 used a United

States internet service provider to communicate.

(5) The connection allowed the balloon to send burst transmissions, or high-bandwidth collections of data over short periods.

(6) Foreign adversaries and affiliated foreign defense companies frequently acquire components and services, sourced from the United States, through violation of United States export control laws.

(b) Supply Chain Risk Mitigation.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in collaboration with such heads of elements of the intelligence community as the Director considers appropriate, develop and commence implementation of a strategy to work with United States companies to mitigate or disrupt the acquisition and use of United States components in the conduct of activities harmful to the national security of the United States.

(c) Goal.—The goal of the strategy required by subsection (b) shall be to inform and provide intelligence support to government and private sector entities in preventing United States components and technologies from aiding or supporting hostile or harmful activities conducted by foreign adversaries of the United States.

(d) Consultation.—In developing and implementing the strategy required by subsection (b), the Director of National Intelligence—

(1) shall consult with the Secretary of Commerce, the Secretary of Defense, and the Secretary of Homeland Security; and

(2) may consult with such other heads of Federal departments or agencies as the Director of National Intelligence considers appropriate.

(e) Annual Reports.—Not later than 1 year after the date of the enactment of this Act and annually thereafter until the date that is 3 years after the date of the enactment of this Act, the Director shall submit to Congress an annual report on the status and effect of the implementation of the strategy required by subsection (b).

SEC. 435. OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE REVIEW OF VISITORS AND ASSIGNEES.

(a) Definitions.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Select Committee on Intelligence and the Committee on Energy and Natural Resources of the Senate; and

(B) the Permanent Select Committee on Intelligence and the Committee on Energy and Commerce of the House of Representatives.

(2) ASSIGNEE; VISITOR.—The terms "assignee" and "visitor" mean a foreign national from a country identified in the report submitted to Congress by the Director of National

Intelligence in 2024 pursuant to section 108B of the National Security Act of 1947 (50 U.S.C. 3043b) (commonly referred to as the "Annual Threat Assessment") as "engaging in competitive behavior that directly threatens U.S. national security", who is not an employee of a National Laboratory, and has requested access to the premises, information, or technology of a National Laboratory.

(3) DIRECTOR.—The term "Director" means the Director of the Office of Intelligence and Counterintelligence of the Department of Energy (or their designee).

(4) FOREIGN NATIONAL.—The term "foreign national" has the meaning given the term "alien" in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(5) NATIONAL LABORATORY.—The term "National Laboratory" has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(6) NON-TRADITIONAL COLLECTOR.—The term "non-traditional collector" means an individual not employed by a foreign intelligence service, who is seeking access to sensitive information about a capability, research, or organizational dynamics of the United States to inform a foreign adversary or non-state actor.

(b) Findings.—The Senate finds the following:

(1) The National Laboratories conduct critical, cutting-edge research across a range of scientific disciplines that provide the United States with a technological edge over other countries.

(2) The technologies developed in the National Laboratories contribute to the national security of the United States, including classified and sensitive military technology and dual-use commercial technology.

(3) International cooperation in the field of science is critical to the United States maintaining its leading technological edge.

(4) The research enterprise of the Department of Energy, including the National Laboratories, is increasingly targeted by adversarial nations to exploit military and dual-use technologies for military or economic gain.

(5) Approximately 40,000 citizens of foreign countries, including more than 8,000 citizens from China and Russia, were granted access to the premises, information, or technology of National Laboratories in fiscal year 2023.

(6) The Office of Intelligence and Counterintelligence of the Department of Energy is responsible for identifying and mitigating counterintelligence risks to the Department, including the National Laboratories.

(c) Sense of the Senate.—It is the sense of the Senate that, before being granted access to the premises, information, or technology of a National Laboratory, citizens of foreign countries identified in the 2024 Annual Threat Assessment of the intelligence community as "engaging in competitive behavior that directly threatens U.S. national security" should be appropriately screened by the National Laboratory to which they seek access, and by the Office of Intelligence and Counterintelligence of the Department, to identify and mitigate risks associated with granting the requested access to sensitive military, or dual-use technologies.

(d) Review of Sensitive Country Visitor and Assignee Access Requests.—The Director shall promulgate a policy to assess the counterintelligence risk each visitor or assignee poses to the research or activities undertaken at a National Laboratory.

(e) Advice With Respect to Visitors or Assignees.—

(1) IN GENERAL.—The Director shall provide advice to a National Laboratory on visitors and assignees when 1 or more of the following conditions are present:

(A) The Director has reason to believe that a visitor or assignee is a non-traditional intelligence collector.

(B) The Director is in receipt of information indicating that a visitor or assignee constitutes a counterintelligence risk to a National Laboratory.

(2) ADVICE DESCRIBED.—Advice provided to a National Laboratory in accordance with paragraph (1) shall include—

(A) a description of the assessed risk;

(B) recommendations to mitigate the risk; and

(C) identification of research or technology that would be at risk if access is granted to the visitor or assignee concerned.

(f) Reports to Congress.—Not later than 90 days after the date of the enactment of this Act, and quarterly thereafter, the Director shall submit to the appropriate congressional committees a report, which shall include—

(1) the number of visitors or assignees permitted to access the premises, information, or technology of each National Laboratory;

(2) the number of instances in which the Director advised a National Laboratory in accordance with subsection (e); and

(3) the number of instances in which a National Laboratory admitted a visitor or assignee against the advice of the Director.

SEC. 436. PROHIBITION ON NATIONAL LABORATORIES ADMITTING CERTAIN FOREIGN NATIONALS.

(a) Definitions.—In this section:

(1) ASSIGNEE.—The term “assignee” means an individual who is seeking approval from, or has been approved by, a National Laboratory to access the premises, information, or technology of the National Laboratory for a period of more than 30 consecutive days.

(2) COVERED FOREIGN NATIONAL.—

(A) IN GENERAL.—The term “covered foreign national” means a foreign national of any of the following countries:

(i) The People’s Republic of China.

(ii) The Russian Federation.

(iii) The Islamic Republic of Iran.

(iv) The Democratic People's Republic of Korea.

(v) The Republic of Cuba.

(B) EXCLUSION.—The term "covered foreign national" does not include an individual that is lawfully admitted for permanent residence (as defined in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a))).

(3) FOREIGN NATIONAL.—The term "foreign national" has the meaning given the term "alien" in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)).

(4) NATIONAL LABORATORY.—The term "National Laboratory" has the meaning given the term in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(5) SENIOR COUNTERINTELLIGENCE OFFICIAL.—The term "senior counterintelligence official" means—

(A) the Director of the Federal Bureau of Investigation;

(B) the Deputy Director of the Federal Bureau of Investigation;

(C) the Executive Assistant Director of the National Security Branch of the Federal Bureau of Investigation; or

(D) the Assistant Director of the Counterintelligence Division of the Federal Bureau of Investigation.

(6) VISITOR.—The term "visitor" means an individual who is seeking approval from, or has been approved by, a National Laboratory to access the premises, information, or technology of the National Laboratory for any period shorter than a period described in paragraph (1).

(b) Prohibition.—

(1) IN GENERAL.—Except as provided in paragraph (2), beginning on the date of enactment of this Act, a National Laboratory—

(A) shall not admit as a visitor or assignee any covered foreign national; and

(B) shall prohibit access to any visitor or assignee that is a covered foreign national and has sought or obtained approval to access the premises, information, or technology of the National Laboratory as of that date.

(2) WAIVER.—Paragraph (1) shall not apply to a National Laboratory if the Secretary of Energy, in consultation with the Director of the Office of Intelligence and Counterintelligence of the Department of Energy and a senior counterintelligence official, certifies and issues a waiver to the National Laboratory requesting to admit a covered foreign national as a visitor or assignee, in writing, that the benefits to the United States of admittance or access by that covered foreign national outweigh the national security and economic risks to the United States.

(3) NOTIFICATION TO CONGRESS.—Not later than 30 days after the date that a waiver is issued pursuant to paragraph (2), the Secretary of Energy shall submit to the Select

Committee on Intelligence of the Senate, the Committee on Energy and Natural Resources of the Senate, the Committee on Commerce, Science, and Transportation of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on Energy and Commerce of the House of Representatives, and the Committee on Science, Space, and Technology of the House of Representatives a notification describing each waiver issued pursuant to paragraph (2), including—

(A) the country of origin of the covered foreign national who is the subject of the waiver;

(B) the date of the request by the covered foreign national for admission or access to a National Laboratory;

(C) the date on which the decision to issue the waiver was made; and

(D) the specific reasons for issuing the waiver.

SEC. 437. QUARTERLY REPORT ON CERTAIN FOREIGN NATIONALS ENCOUNTERED AT THE UNITED STATES BORDER.

(a) Definitions.—In this section:

(1) ENCOUNTERED.—The term "encountered", with respect to a special interest alien, means physically apprehended by U.S. Customs and Border Protection personnel.

(2) SPECIAL INTEREST ALIEN.—The term "special interest alien" means an alien (as defined in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)) who, based upon an analysis of travel patterns and other information available to the United States Government, potentially poses a threat to the national security of the United States and its interests due to a known or potential nexus to terrorism, espionage, organized crime, or other malign actors.

(b) In General.—Not later than 60 days after the date of the enactment of this Act, and quarterly thereafter for the following 3 years, the Secretary of Homeland Security, in coordination with the Director of National Intelligence, shall publish, on a publicly accessible website of the Department of Homeland Security, a report identifying the aggregate number of special interest aliens who, during the applicable reporting period—

(1) have been encountered at or near an international border of the United States; and

(2)(A) have been released from custody;

(B) are under supervision;

(C) are being detained by the Department of Homeland Security; or

(D) have been removed from the United States.

SEC. 438. ASSESSMENT OF THE LESSONS LEARNED BY THE INTELLIGENCE COMMUNITY WITH RESPECT TO

THE ISRAEL-HAMAS WAR.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with such other heads of elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress a written assessment of the lessons learned from the Israel-Hamas war.

(b) Elements.—The assessment required by subsection (a) shall include the following:

(1) Lessons learned from the timing and scope of the October 7, 2023 attack by Hamas against Israel, including lessons related to United States intelligence cooperation with Israel and other regional partners.

(2) Lessons learned from advances in warfare, including the use by adversaries of a complex tunnel network.

(3) Lessons learned from attacks by adversaries against maritime shipping routes in the Red Sea.

(4) Lessons learned from the use by adversaries of rockets, missiles, and unmanned aerial systems, including attacks by Iran.

(5) Analysis of the impact of the Israel-Hamas war on the global security environment, including the war in Ukraine.

(c) Form.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) Appropriate Committees of Congress Defined.—In this section, the term "appropriate committees of Congress" means—

(1) the congressional intelligence committees;

(2) the Committee on Armed Services and the Committee on Appropriations of the Senate; and

(3) the Committee on Armed Services and the Committee on Appropriations of the House of Representatives.

SEC. 439. CENTRAL INTELLIGENCE AGENCY INTELLIGENCE ASSESSMENT ON TREN DE ARAGUA.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency, in consultation with such other heads of elements of the intelligence community as the Director considers appropriate, shall submit to the appropriate committees of Congress an intelligence assessment on the gang known as "Tren de Aragua".

(b) Elements.—The intelligence assessment required by subsection (a) shall include the following:

(1) A description of the key leaders, organizational structure, subgroups, presence in countries in the Western Hemisphere, and cross-border illicit drug smuggling routes of Tren de Aragua.

(2) A description of the practices used by Tren de Aragua to generate revenue.

(3) A description of the level at which Tren de Aragua receives support from the regime of Nicolas Maduro in Venezuela.

(4) A description of the manner in which Tren de Aragua is exploiting heightened migratory flows out of Venezuela and throughout the Western Hemisphere to expand its operations.

(5) A description of the degree to which Tren de Aragua cooperates or competes with other criminal organizations in the Western Hemisphere.

(6) An estimate of the annual revenue received by Tren de Aragua from the sale of illicit drugs, kidnapping, and human trafficking, disaggregated by activity.

(7) A determination on whether Tren De Aragua meets the definition of "significant transnational criminal organization" in section 3 of Executive Order 13581 (76 Fed. Reg. 44757; relating to blocking property of transnational criminal organizations), as amended by Executive Order 13863 (84 Fed. Reg. 10255; relating to taking additional steps to address the national emergency with respect to significant transnational criminal organizations).

(8) Any other information the Director of the Central Intelligence Agency considers relevant.

(c) Form.—The intelligence assessment required by subsection (a) may be submitted in classified form.

(d) Definition of Appropriate Committees of Congress.—In this section, the term "appropriate committees of Congress" means—

(1) the congressional intelligence committees;

(2) the Committee on Foreign Relations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, and the Committee on Appropriations of the Senate; and

(3) the Committee on Foreign Affairs, the Committee on Homeland Security, and the Committee on Appropriations of the House of Representatives.

SEC. 440. ASSESSMENT OF MADURO REGIME'S ECONOMIC AND SECURITY RELATIONSHIPS WITH STATE SPONSORS OF TERRORISM AND FOREIGN TERRORIST ORGANIZATIONS.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees a written assessment of the economic and security relationships of the regime of Nicolas Maduro of Venezuela with the countries and organizations described in subsection (b), including formal and informal support to and from such countries and organizations.

(b) Countries and Organizations Described.—The countries and organizations described in this subsection are the following:

(1) The following countries designated by the United States as state sponsors of terrorism:

(A) The Republic of Cuba.

(B) The Islamic Republic of Iran.

(2) The following organizations designated by the United States as foreign terrorist organizations:

(A) The National Liberation Army (ELN).

(B) The Revolutionary Armed Forces of Colombia–People's Army (FARC-EP).

(C) The Segunda Marquetalia.

(c) Form.—The assessment required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 441. CONTINUED CONGRESSIONAL OVERSIGHT OF IRANIAN EXPENDITURES SUPPORTING FOREIGN MILITARY AND TERRORIST ACTIVITIES.

(a) Update Required.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall submit to the congressional intelligence committees an update to the report submitted under section 6705 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) to reflect current occurrences, circumstances, and expenditures.

(b) Form.—The update submitted pursuant to subsection (a) shall be submitted in unclassified form, but may include a classified annex.

TITLE V—EMERGING TECHNOLOGIES

SEC. 501. STRATEGY TO COUNTER FOREIGN ADVERSARY EFFORTS TO UTILIZE BIOTECHNOLOGIES IN WAYS THAT THREATEN UNITED STATES NATIONAL SECURITY.

(a) Sense of Congress.—It is the sense of Congress that as biotechnologies become increasingly important with regard to the national security interests of the United States, and with the addition of biotechnologies to the biosecurity mission of the National Counterproliferation and Biosecurity Center, the intelligence community must articulate and implement a whole-of-government strategy for addressing concerns relating to biotechnologies.

(b) Strategy for Biotechnologies Critical to National Security.—

(1) STRATEGY REQUIRED.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall, acting through the Director of the National Counterproliferation and Biosecurity Center and in coordination with the heads of such

other elements of the intelligence community as the Director of National Intelligence considers appropriate, develop and submit to the congressional intelligence committees a whole-of-government strategy to address concerns relating to biotechnologies.

(2) ELEMENTS.—The strategy developed and submitted pursuant to paragraph (1) shall include the following:

(A) Identification and assessment of biotechnologies critical to the national security of the United States, including an assessment of which materials involve a dependency on foreign adversary nations.

(B) A determination of how best to counter foreign adversary efforts to utilize biotechnologies that threaten the national security of the United States, including technologies identified pursuant to paragraph (1).

(C) A plan to support United States efforts and capabilities to secure the United States supply chains of the technologies identified pursuant to paragraph (1), by coordinating—

(i) across the intelligence community;

(ii) the support provided by the intelligence community to other relevant Federal agencies and policymakers;

(iii) the engagement of the intelligence community with private sector entities; and

(iv) how the intelligence community can support securing United States supply chains for and use of biotechnologies.

(D) Proposals for such legislative or administrative action as the Directors consider necessary to support the strategy.

SEC. 502. IMPROVEMENTS TO THE ROLES, MISSIONS, AND OBJECTIVES OF THE NATIONAL COUNTERPROLIFERATION AND BIOSECURITY CENTER.

Section 119A of the National Security Act of 1947 (50 U.S.C. 3057) is amended—

(1) in subsection (a)(4), by striking "biosecurity and" and inserting "counterproliferation, biosecurity, and"; and

(2) in subsection (b)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking "analyzing and";

(ii) in subparagraph (C), by striking "Establishing" and inserting "Coordinating the establishment of";

(iii) in subparagraph (D), by striking "Disseminating" and inserting

"Overseeing the dissemination of";

(iv) in subparagraph (E), by inserting "and coordinating" after "Conducting"; and

(v) in subparagraph (G), by striking "Conducting" and inserting "Coordinating and advancing"; and

(B) in paragraph (2)—

(i) in subparagraph (B), by striking "and analysis";

(ii) by redesignating subparagraphs (C) through (E) as subparagraphs (D) through (F), respectively;

(iii) by inserting after subparagraph (B) the following:

"(C) Overseeing and coordinating the analysis of intelligence on biosecurity and foreign biological threats in support of the intelligence needs of Federal departments and agencies responsible for public health, including by providing analytic priorities to elements of the intelligence community and by conducting and coordinating net assessments.";

(iv) in subparagraph (D), as redesignated by clause (ii), by inserting "on matters relating to biosecurity and foreign biological threats" after "public health";

(v) in subparagraph (F), as redesignated by clause (ii), by inserting "and authorities" after "capabilities"; and

(vi) by adding at the end the following:

"(G) Coordinating with relevant elements of the intelligence community and other Federal departments and agencies responsible for public health to engage with private sector entities on information relevant to biosecurity, biotechnology, and foreign biological threats.".

SEC. 503. ENHANCING CAPABILITIES TO DETECT FOREIGN ADVERSARY THREATS RELATING TO BIOLOGICAL DATA.

Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the heads of such Federal departments and agencies as the Director considers appropriate, take the following steps to standardize and enhance the capabilities of the intelligence community to detect foreign adversary threats relating to biological data:

(1) Prioritize the collection, analysis, and dissemination of information relating to foreign adversary use of biological data, particularly in ways that threaten or could threaten the national security of the United States.

(2) Issue policy guidance within the intelligence community—

(A) to standardize the handling and processing of biological data, including with

respect to protecting the civil liberties and privacy of United States persons;

(B) to standardize and enhance intelligence engagements with foreign allies and partners with respect to biological data; and

(C) to standardize the creation of metadata relating to biological data.

(3) Ensure coordination with such Federal departments and agencies and entities in the private sector as the Director considers appropriate to understand how foreign adversaries are accessing and using biological data stored within the United States.

SEC. 504. NATIONAL SECURITY PROCEDURES TO ADDRESS CERTAIN RISKS AND THREATS RELATING TO ARTIFICIAL INTELLIGENCE.

(a) Findings.—Congress finds the following:

(1) Artificial intelligence systems demonstrate increased capabilities in the generation of synthetic media and computer programming code, as well as areas such as object recognition, natural language processing, and workflow orchestration.

(2) The growing capabilities of artificial intelligence systems in the areas described in paragraph (1), as well as the greater accessibility of large-scale artificial intelligence models and advanced computation capabilities to individuals, businesses, and governments, have dramatically increased the adoption of artificial intelligence products in the United States and globally.

(3) The advanced capabilities of the systems described in paragraph (1), and their accessibility to a wide-range of users, have increased the likelihood and effect of misuse or malfunction of these systems, such as to generate synthetic media for disinformation campaigns, develop or refine malware for computer network exploitation activity, enhance surveillance capabilities in ways that undermine the privacy of citizens of the United States, and increase the risk of exploitation or malfunction of information technology systems incorporating artificial intelligence systems in mission-critical fields such as health care, critical infrastructure, and transportation.

(b) Procedures Required.—Not later than 180 days after the date of the enactment of this Act, the President shall develop and issue procedures to facilitate and promote mechanisms by which—

(1) vendors of advanced computation capabilities, vendors and commercial users of artificial intelligence systems, as well as independent researchers and other third parties, may effectively notify appropriate elements of the United States Government of—

(A) information security risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system to develop or refine malicious software;

(B) information security risks such as indications of compromise or other threat information indicating a compromise to the confidentiality, integrity, or availability of an artificial intelligence system, or to the supply chain of an artificial intelligence system, including training or test data, frameworks, computing environments, or other

components necessary for the training, management, or maintenance of an artificial intelligence system;

(C) biosecurity risks emanating from artificial intelligence systems, such as the use of an artificial intelligence system to design, develop, or acquire dual-use biological entities such as putatively toxic small molecules, proteins, or pathogenic organisms;

(D) suspected foreign malign influence (as defined by section 119C of the National Security Act of 1947 (50 U.S.C. 3059(f))) activity that appears to be facilitated by an artificial intelligence system; and

(E) any other unlawful activity facilitated by, or directed at, an artificial intelligence system;

(2) elements of the Federal Government may provide threat briefings to vendors of advanced computation capabilities and vendors of artificial intelligence systems, alerting them, as may be appropriate, to potential or confirmed foreign exploitation of their systems, as well as malign foreign plans and intentions.

(c) Briefing Required.—

(1) APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term "appropriate committees of Congress" means—

(A) the congressional intelligence committees;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(C) the Committee on Homeland Security of the House of Representatives.

(2) IN GENERAL.—The President shall provide the appropriate committees of Congress a briefing on procedures developed and issued pursuant to subsection (b).

(3) ELEMENTS.—The briefing provided pursuant to paragraph (2) shall include the following:

(A) A clear specification of which Federal agencies are responsible for leading outreach to affected industry and the public with respect to the matters described in subparagraphs (A) through (E) of paragraph (1) of subsection (b) and paragraph (2) of such subsection.

(B) An outline of a plan for industry outreach and public education regarding risks posed by, and directed at, artificial intelligence systems.

(C) Use of research and development, stakeholder outreach, and risk management frameworks established pursuant to—

(i) provisions of law in effect on the day before the date of the enactment of this Act; or

(ii) Federal agency guidelines.

SEC. 505. ESTABLISHMENT OF ARTIFICIAL

INTELLIGENCE SECURITY CENTER.

(a) Establishment.—Not later than 90 days after the date of the enactment of this Act, the Director of the National Security Agency shall establish an Artificial Intelligence Security Center within the Cybersecurity Collaboration Center of the National Security Agency.

(b) Functions.—The functions of the Artificial Intelligence Security Center shall be as follows:

(1) Making available a research test bed to private sector and academic researchers, on a subsidized basis, to engage in artificial intelligence security research, including through the secure provision of access in a secure environment to proprietary third-party models, with the consent of the vendors of the models.

(2) Developing guidance to prevent or mitigate counter-artificial intelligence techniques.

(3) Promoting secure artificial intelligence adoption practices for managers of national security systems (as defined in section 3552 of title 44, United States Code) and elements of the defense industrial base.

(4) Coordinating with the Artificial Intelligence Safety Institute of the National Institute of Standards and Technology.

(5) Such other functions as the Director considers appropriate.

(c) Test Bed Requirements.—

(1) ACCESS AND TERMS OF USAGE.—

(A) RESEARCHER ACCESS.—The Director shall establish terms of usage governing researcher access to the test bed made available under subsection (b)(1), with limitations on researcher publication only to the extent necessary to protect classified information or proprietary information concerning third-party models provided through the consent of model vendors.

(B) AVAILABILITY TO FEDERAL AGENCIES.—The Director shall ensure that the test bed made available under subsection (b)(1) is also made available to other Federal agencies on a cost-recovery basis.

(2) USE OF CERTAIN INFRASTRUCTURE AND OTHER RESOURCES.—In carrying out subsection (b)(1), the Director shall leverage, to the greatest extent practicable, infrastructure and other resources provided under section 5.2 of the Executive Order dated October 30, 2023 (relating to safe, secure, and trustworthy development and use of artificial intelligence).

(d) Access to Proprietary Models.—In carrying out this section, the Director shall establish such mechanisms as the Director considers appropriate, including potential contractual incentives, to ensure the provision of access to proprietary models by qualified independent third-party researchers if commercial model vendors have voluntarily provided models and associated resources for such testing.

(e) Counter-artificial Intelligence Defined.—In this section, the term "counter-artificial intelligence" means techniques or procedures to extract information about the behavior or

characteristics of an artificial intelligence system, or to learn how to manipulate an artificial intelligence system, in order to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

SEC. 506. SENSE OF CONGRESS ENCOURAGING INTELLIGENCE COMMUNITY TO INCREASE PRIVATE SECTOR CAPITAL PARTNERSHIPS AND PARTNERSHIP WITH OFFICE OF STRATEGIC CAPITAL OF DEPARTMENT OF DEFENSE TO SECURE ENDURING TECHNOLOGICAL ADVANTAGES.

It is the sense of Congress that—

(1) acquisition leaders in the intelligence community should further explore the strategic use of private capital partnerships to secure enduring technological advantages for the intelligence community, including through the identification, development, and transfer of promising technologies to full-scale programs capable of meeting intelligence community requirements; and

(2) the intelligence community should undertake regular consultation with Federal partners, such as the Office of Strategic Capital of the Office of the Secretary of Defense, on best practices and lessons learned from their experiences integrating these resources so as to accelerate attainment of national security objectives.

SEC. 507. INTELLIGENCE COMMUNITY TECHNOLOGY BRIDGE FUND.

(a) Definitions.—In this section:

(1) NONPROFIT ORGANIZATION.—The term "nonprofit organization" means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and that is exempt from tax under section 501(a) of such Code.

(2) WORK PROGRAM.—The term "work program" means any agreement between In-Q-Tel and a third-party company, where such third-party company furnishes or is furnishing a product or service for use by any of In-Q-Tel's government customers to address those customers' technology needs or requirements.

(b) Establishment of Fund.—There is established in the Treasury of the United States a fund to be known as the "Intelligence Community Technology Bridge Fund" (in this subsection referred to as the "Fund") to assist in the transitioning of products or services from the research and development phase to the contracting and production phase.

(c) Contents of Fund.—The Fund shall consist of amounts appropriated to the Fund, and amounts in the Fund shall remain available until expended.

(d) Availability and Use of Fund.—

(1) IN GENERAL.—Subject to paragraph (3), amounts in the Fund shall be available to the

24cv3373_24-02439_000333

Director of National Intelligence to provide assistance to a business or nonprofit organization that is transitioning a product or service.

(2) TYPES OF ASSISTANCE.—Assistance provided under paragraph (1) may be distributed as funds in the form of a grant, a payment for a product or service, or a payment for equity.

(3) REQUIREMENTS FOR FUNDS.—Assistance may be provided under paragraph (1) to a business or nonprofit organization that is transitioning a product or service only if—

(A) the business or nonprofit organization—

(i) has participated or is participating in a work program; or

(ii) is engaged with an element of the intelligence community or Department of Defense for research and development; and

(B) the Director of National Intelligence or the head of an element of the intelligence community attests that the product or service will be utilized by an element of the intelligence community for a mission need, such as because it would be valuable in addressing a needed capability, fill or complement a technology gap, or increase the supplier base or price-competitiveness for the Federal Government.

(4) PRIORITY FOR SMALL BUSINESS CONCERNS AND NONTRADITIONAL DEFENSE CONTRACTORS.—In providing assistance under paragraph (1), the Director shall prioritize the provision of assistance to small business concerns (as defined under section 3(a) of the Small Business Act (15 U.S.C. 632(a))) and nontraditional defense contractors (as defined in section 3014 of title 10, United States Code).

(e) Administration of Fund.—

(1) IN GENERAL.—The Fund shall be administered by the Director of National Intelligence.

(2) CONSULTATION.—In administering the Fund, the Director—

(A) shall consult with the heads of the elements of the intelligence community; and

(B) may consult with In-Q-Tel, the Defense Advanced Research Project Agency, the North Atlantic Treaty Organization Investment Fund, and the Defense Innovation Unit.

(f) Annual Reports.—

(1) IN GENERAL.—Not later than September 30, 2025, and each fiscal year thereafter, the Director shall submit to the congressional intelligence committees a report on the Fund.

(2) CONTENTS.—Each report submitted pursuant to paragraph (1) shall include, for the period covered by the report, information about the following:

(A) How much was expended or obligated using amounts from the Fund.

(B) For what the amounts were expended or obligated.

(C) The effects of such expenditures and obligations.

(D) A summary of annual transition activities and outcomes of such activities for the intelligence community.

(3) FORM.—Each report submitted pursuant to paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(g) Authorization of Appropriations.—

(1) IN GENERAL.—Subject to paragraph (2), there is authorized to be appropriated to the Fund $75,000,000 for fiscal year 2025 and for each fiscal year thereafter.

(2) LIMITATION.—The amount in the Fund shall not exceed $75,000,000 at any time.

SEC. 508. ENHANCEMENT OF AUTHORITY FOR INTELLIGENCE COMMUNITY PUBLIC-PRIVATE TALENT EXCHANGES.

(a) Focus Areas.—Subsection (a) of section 5306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334) is amended—

(1) by striking "Not later than" and inserting the following:

"(1) IN GENERAL.—Not later than"; and

(2) by adding at the end the following:

"(2) FOCUS AREAS.—The Director shall ensure that the policies, processes, and procedures developed pursuant to paragraph (1) include a focus on rotations described in such paragraph with private-sector organizations in the following fields:

"(A) Finance.

"(B) Acquisition.

"(C) Biotechnology.

"(D) Computing.

"(E) Artificial intelligence.

"(F) Business process innovation and entrepreneurship.

"(G) Cybersecurity.

"(H) Materials and manufacturing.

"(I) Any other technology or research field the Director determines relevant to meet evolving national security threats in technology sectors.".

(b) Duration of Temporary Details.—Subsection (e) of section 5306 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334) is amended—

(1) in paragraph (1), by striking "3 years" and inserting "5 years"; and

(2) in paragraph (2), by striking "3 years" and inserting "5 years".

(c) Treatment of Private-sector Employees.—Subsection (g) of such section is amended—

(1) in paragraph (5), by striking "; and" and inserting a semicolon;

(2) in paragraph (6), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(7) shall not be considered to have a conflict of interest with an element of the intelligence community solely because of being detailed to an element of the intelligence community under this section.".

(d) Hiring Authority.—Such section is amended—

(1) by redesignating subsection (j) as subsection (k); and

(2) by inserting after subsection (i) the following:

"(j) Hiring Authority.—

"(1) IN GENERAL.—The Director may hire, under section 213.3102(r) of title 5, Code of Federal Regulations, or successor regulations, an individual who is an employee of a private-sector organization who is detailed to an element of the intelligence community under this section.

"(2) NO PERSONNEL BILLET REQUIRED.—Hiring an individual under paragraph (1) shall not require a personnel billet.".

(e) Annual Reports.—Not later than 1 year after the date of the enactment of this Act and annually thereafter for 2 more years, the Director of National Intelligence shall submit to the congressional intelligence committees an annual report on—

(1) the implementation of the policies, processes, and procedures developed pursuant to subsection (a) of such section 5306 (50 U.S.C. 3334) and the administration of such section;

(2) how the heads of the elements of the intelligence community are using or plan to use the authorities provided under such section; and

(3) recommendations for legislative or administrative action to increase use of the authorities provided under such section.

SEC. 509. ENHANCING INTELLIGENCE COMMUNITY ABILITY TO ACQUIRE EMERGING TECHNOLOGY THAT FULFILLS INTELLIGENCE COMMUNITY NEEDS.

(a) Definition of Work Program.—The term "work program" means any agreement between In-Q-Tel and a third-party company, where such third-party company furnishes or is furnishing a property, product, or service for use by any of In-Q-Tel's government customers to address those customers' technology needs or requirements.

(b) In General.—In addition to the exceptions listed under section 3304(a) of title 41, United States Code, and under section 3204(a) of title 10, United States Code, for the use of competitive procedures, the Director of National Intelligence or the head of an element of the intelligence community may use procedures other than competitive procedures to acquire a property, product, or service if—

(1) the source of the property, product, or service is a company that completed a work program in which the company furnished the property, product, or service; and

(2) the Director of National Intelligence or the head of an element of the intelligence community certifies that such property, product, or service has been shown to meet an identified need of the intelligence community.

(c) Justification for Use of Procedures Other Than Competitive Procedures.—

(1) IN GENERAL.—A property, product, or service may not be acquired by the Director or the head of an element of the intelligence community under subsection (b) using procedures other than competitive procedures unless the acquiring officer for the acquisition justifies the use of such procedures in writing.

(2) CONTENTS.—A justification in writing described in paragraph (1) for an acquisition using procedures other than competitive procedures shall include the following:

(A) A description of the need of the element of the intelligence community that the property, product, or service satisfies.

(B) A certification that the anticipated costs will be fair and reasonable.

(C) A description of the market survey conducted or a statement of the reasons a market survey was not conducted.

(D) Such other matters as the Director or the head, as the case may be, determines appropriate.

SEC. 510. MANAGEMENT OF ARTIFICIAL INTELLIGENCE SECURITY RISKS.

(a) Definitions.—In this section:

(1) ARTIFICIAL INTELLIGENCE SAFETY INCIDENT.—The term "artificial intelligence safety incident" means an event that increases the risk that operation of an artificial intelligence system will—

(A) result in physical or psychological harm; or

(B) lead to a state in which human life, health, property, or the environment is endangered.

(2) ARTIFICIAL INTELLIGENCE SECURITY INCIDENT.—The term "artificial intelligence security incident" means an event that increases—

(A) the risk that operation of an artificial intelligence system occurs in a way that enables the extraction of information about the behavior or characteristics of an artificial intelligence system by a third party; or

(B) the ability of a third party to manipulate an artificial intelligence system to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

(3) ARTIFICIAL INTELLIGENCE SECURITY VULNERABILITY.—The term "artificial

intelligence security vulnerability" means a weakness in an artificial intelligence system that could be exploited by a third party to, without authorization, subvert the confidentiality, integrity, or availability of an artificial intelligence system, including through techniques such as—

(A) data poisoning;

(B) evasion attacks;

(C) privacy-based attacks; and

(D) abuse attacks.

(4) COUNTER-ARTIFICIAL INTELLIGENCE.—The term "counter-artificial intelligence" means techniques or procedures to extract information about the behavior or characteristics of an artificial intelligence system, or to learn how to manipulate an artificial intelligence system, so as to subvert the confidentiality, integrity, or availability of an artificial intelligence system or adjacent system.

(b) Voluntary Tracking and Processing of Security and Safety Incidents and Risks Associated With Artificial Intelligence.—

(1) PROCESSES AND PROCEDURES FOR VULNERABILITY MANAGEMENT.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall—

(A) initiate a process to update processes and procedures associated with the National Vulnerability Database of the Institute to ensure that the database and associated vulnerability management processes incorporate artificial intelligence security vulnerabilities to the greatest extent practicable; and

(B) identify any characteristics of artificial intelligence security vulnerabilities that make utilization of the National Vulnerability Database inappropriate for their management and develop processes and procedures for vulnerability management of those vulnerabilities.

(2) VOLUNTARY TRACKING OF ARTIFICIAL INTELLIGENCE SECURITY AND ARTIFICIAL INTELLIGENCE SAFETY INCIDENTS.—

(A) VOLUNTARY DATABASE REQUIRED.—Not later than 1 year after the date of the enactment of this Act, the Director of the Institute, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(i) develop and establish a comprehensive database to publicly track artificial intelligence security and artificial intelligence safety incidents through voluntary input; and

(ii) in establishing the database under clause (i)—

(I) establish mechanisms by which private sector entities, public sector organizations, civil society groups, and academic researchers may voluntarily share information with the Institute on confirmed or suspected artificial intelligence security or artificial intelligence safety incidents, in a manner that preserves the confidentiality of any affected party;

(II) leverage, to the greatest extent possible, standardized disclosure and incident description formats;

(III) develop processes to associate reports pertaining to the same incident with a single incident identifier;

(IV) establish classification, information retrieval, and reporting mechanisms that sufficiently differentiate between artificial intelligence security incidents and artificial intelligence safety incidents; and

(V) create appropriate taxonomies to classify incidents based on relevant characteristics, impact, or other relevant criteria.

(B) IDENTIFICATION AND TREATMENT OF MATERIAL ARTIFICIAL INTELLIGENCE SECURITY OR ARTIFICIAL INTELLIGENCE SAFETY RISKS.—

(i) IN GENERAL.—Upon receipt of relevant information on an artificial intelligence security or artificial intelligence safety incident, the Director of the Institute shall determine whether the described incident presents a material artificial intelligence security or artificial intelligence safety risk sufficient for inclusion in the database developed and established under subparagraph (A).

(ii) PRIORITIES.—In evaluating a reported incident pursuant to subparagraph (A), the Director shall prioritize inclusion in the database cases in which a described incident—

(I) describes an artificial intelligence system used in critical infrastructure or safety-critical systems;

(II) would result in a high-severity or catastrophic impact to the people or economy of the United States; or

(III) includes an artificial intelligence system widely used in commercial or public sector contexts.

(C) REPORTS AND ANONYMITY.—The Director shall populate the database developed and established under subparagraph (A) with incidents based on public reports and information shared using the mechanism established pursuant to clause (ii)(I) of such subparagraph, ensuring that any incident description sufficiently anonymizes those affected, unless those who are affected have consented to their names being included in the database.

(c) Updating Processes and Procedures Relating to Common Vulnerabilities and Exposures Program and Evaluation of Consensus Standards Relating to Artificial Intelligence Security Vulnerability Reporting.—

(1) DEFINITIONS.—In this subsection:

(A) COMMON VULNERABILITIES AND EXPOSURES PROGRAM.—The term "Common Vulnerabilities and Exposures Program" means the reference guide and classification system for publicly known information security vulnerabilities sponsored by the Cybersecurity and Infrastructure Security Agency.

(B) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and

Infrastructure Security Agency.

(C) RELEVANT CONGRESSIONAL COMMITTEES.—The term "relevant congressional committees" means—

(i) the Committee on Homeland Security and Governmental Affairs of the Senate;

(ii) the Committee on Commerce, Science, and Transportation of the Senate;

(iii) the Select Committee on Intelligence of the Senate;

(iv) the Committee on the Judiciary of the Senate;

(v) the Committee on Oversight and Accountability of the House of Representatives;

(vi) the Committee on Energy and Commerce of the House of Representatives;

(vii) the Permanent Select Committee on Intelligence of the House of Representatives; and

(viii) the Committee on the Judiciary of the House of Representatives.

(2) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director shall—

(A) initiate a process to update processes and procedures associated with the Common Vulnerabilities and Exposures Program to ensure that the program and associated processes identify and enumerate artificial intelligence security vulnerabilities to the greatest extent practicable; and

(B) identify any characteristic of artificial intelligence security vulnerabilities that makes utilization of the Common Vulnerabilities and Exposures Program inappropriate for their management and develop processes and procedures for vulnerability identification and enumeration of those artificial intelligence security vulnerabilities.

(3) EVALUATION OF CONSENSUS STANDARDS.—

(A) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, the Director of the National Institute of Standards and Technology shall initiate a multi-stakeholder process to evaluate whether existing voluntary consensus standards for vulnerability reporting effectively accommodate artificial intelligence security vulnerabilities.

(B) REPORT.—

(i) SUBMISSION.—Not later than 180 days after the date on which the evaluation under subparagraph (A) is carried out, the Director shall submit a report to the relevant congressional committees on the sufficiency of existing vulnerability reporting processes and standards to accommodate artificial intelligence security vulnerabilities.

(ii) POST-REPORT ACTION.—If the Director concludes in the report submitted under clause (i) that existing processes do not sufficiently accommodate reporting

of artificial intelligence security vulnerabilities, the Director shall initiate a process, in consultation with the Director of the National Institute of Standards and Technology and the Director of the Office of Management and Budget, to update relevant vulnerability reporting processes, including the Department of Homeland Security Binding Operational Directive 20–01, or any subsequent directive.

(4) BEST PRACTICES.—Not later than 90 days after the date of enactment of this Act, the Director shall, in collaboration with the Director of the National Security Agency and the Director of the National Institute of Standards and Technology and leveraging efforts of the Information Communications Technology Supply Chain Risk Management Task Force to the greatest extent practicable, convene a multi-stakeholder process to encourage the development and adoption of best practices relating to addressing supply chain risks associated with training and maintaining artificial intelligence models, which shall ensure consideration of supply chain risks associated with—

(A) data collection, cleaning, and labeling, particularly the supply chain risks of reliance on remote workforce and foreign labor for such tasks;

(B) inadequate documentation of training data and test data storage, as well as limited provenance of training data;

(C) human feedback systems used to refine artificial intelligence systems, particularly the supply chain risks of reliance on remote workforce and foreign labor for such tasks;

(D) the use of large-scale, open-source datasets, particularly the supply chain risks to repositories that host such datasets for use by public and private sector developers in the United States; and

(E) the use of proprietary datasets containing sensitive or personally identifiable information.

SEC. 511. PROTECTION OF TECHNOLOGICAL MEASURES DESIGNED TO VERIFY AUTHENTICITY OR PROVENANCE OF MACHINE-MANIPULATED MEDIA.

(a) Definitions.—In this section:

(1) MACHINE-MANIPULATED MEDIA.—The term "machine-manipulated media" has the meaning given such term in section 5724 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (Public Law 116–92; 50 U.S.C. 3024 note).

(2) STATE.—The term "State" means each of the several States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

(b) Prohibitions.—

(1) PROHIBITION ON CONCEALING SUBVERSION.—No person shall knowingly and with the

intent or substantial likelihood of deceiving a third party, enable, facilitate, or conceal the subversion of a technological measure designed to verify the authenticity, modifications, or conveyance of machine-manipulated media, or characteristics of the provenance of the machine-manipulated media, by generating information about the authenticity of a piece of content that is knowingly false.

(2) PROHIBITION ON FRAUDULENT DISTRIBUTION.—No person shall knowingly and for financial benefit, enable, facilitate, or conceal the subversion of a technological measure described in paragraph (1) by distributing machine-manipulated media with knowingly false information about the authenticity of a piece of machine-manipulated media.

(3) PROHIBITION ON PRODUCTS AND SERVICES FOR CIRCUMVENTION.—No person shall deliberately manufacture, import, or offer to the public a technology, product, service, device, component, or part thereof that—

(A) is primarily designed or produced and promoted for the purpose of circumventing, removing, or otherwise disabling a technological measure described in paragraph (1) with the intent or substantial likelihood of deceiving a third party about the authenticity of a piece of machine-manipulated media;

(B) has only limited commercially significant or expressive purpose or use other than to circumvent, remove, or otherwise disable a technological measure designed to verify the authenticity of machine-manipulated media and is promoted for such purposes; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing, removing, or otherwise disabling a technological measure described in paragraph (1) with an intent to deceive a third party about the authenticity of a piece of machine-manipulated media.

(c) Exemptions.—

(1) IN GENERAL.—Nothing in subsection (b) shall inhibit the ability of any individual to access, read, or review a technological measure described in paragraph (1) of such subsection or to access, read, or review the provenance, modification, or conveyance information contained therein.

(2) EXEMPTION FOR NONPROFIT LIBRARIES, ARCHIVES, AND EDUCATIONAL INSTITUTIONS.—

(A) IN GENERAL.—Except as otherwise provided in this subsection, subsection (b) shall not apply to a nonprofit library, archives, or educational institution which generates, distributes, or otherwise handles machine-manipulated media.

(B) COMMERCIAL ADVANTAGE, FINANCIAL GAIN, OR TORTIOUS CONDUCT.—The exception in subparagraph (A) shall not apply to a nonprofit library, archive, or educational institution that willfully for the purpose of commercial advantage, financial gain, or in furtherance of tortious conduct violates a provision of subsection (b), except that a nonprofit library, archive, or educational institution that willfully for the purpose of commercial advantage, financial gain, or in furtherance of tortious conduct violates a provision of subsection (b) shall—

(i) for the first offense, be subject to the civil remedies under subsection (d); and

(ii) for repeated or subsequent offenses, in addition to the civil remedies under subsection (d), forfeit the exemption provided under subparagraph (A).

(C) CIRCUMVENTING TECHNOLOGIES.—This paragraph may not be used as a defense to a claim under paragraph (3) of subsection (b), nor may this subsection permit a nonprofit library, archive, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, that circumvents a technological measure described in paragraph (1) of such subsection.

(D) QUALIFICATIONS OF LIBRARIES AND ARCHIVES.—In order for a library or archive to qualify for the exemption under subparagraph (A), the collections of that library or archive shall be—

(i) open to the public; or

(ii) available not only to researchers affiliated with the library or archive or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(3) REVERSE ENGINEERING.—

(A) DEFINITIONS.—In this paragraph:

(i) CIRCUMVENTION.—The term "circumvention" means to remove, deactivate, disable, or impair a technological measure designed to verify the authenticity of machine-manipulated media or characteristics of its provenance, modifications, or conveyance.

(ii) INTEROPERABILITY.—The term "interoperability" means the ability of—

(I) computer programs to exchange information; and

(II) such programs mutually to use the information which has been exchanged.

(B) IN GENERAL.—An authorized user of a technological measure described in subsection (b)(1) may circumvent such technological measure for the sole purpose of identifying and analyzing those elements of the technological measure that are necessary to achieve interoperability with that authorized user's own technological measures intended for similar purposes of verifying the authenticity of machine-manipulated media or characteristics of its provenance, modifications, or conveyance.

(C) LAW ENFORCEMENT, INTELLIGENCE, AND OTHER GOVERNMENT ACTIVITIES.—Subsection (b) does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State.

(d) Enforcement by Attorney General.—

(1) CIVIL ACTIONS.—The Attorney General may bring a civil action in an appropriate United States district court against any person who violates subsection (b).

(2) POWERS OF THE COURT.—In an action brought under paragraph (1), the court—

(A) may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation, but in no event shall impose a prior restraint on free speech or the press protected under the First Amendment to the Constitution of the United States;

(B) at any time while an action is pending, may order the impounding, on such terms as it deems reasonable, of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation;

(C) may award damages under paragraph (3);

(D) in its discretion may allow the recovery of costs against any party other than the United States or an officer thereof; and

(E) may, as part of a final judgment or decree finding a violation, order the remedial modification or the destruction of any device or product involved in the violation that is in the custody or control of the violator or has been impounded under subparagraph (B).

(3) AWARD OF DAMAGES.—

(A) IN GENERAL.—Except as otherwise provided in this section, a person committing a violation of subsection (b) is liable for statutory damages as provided in subparagraph (C).

(B) STATUTORY DAMAGES.—

(i) ELECTION OF AMOUNT BASED ON NUMBER OF ACTS OF CIRCUMVENTION.—At any time before final judgment is entered, the Attorney General may elect to recover an award of statutory damages for each violation of subsection (b) in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.

(ii) ELECTION OF AMOUNT; TOTAL AMOUNT.—At any time before final judgment is entered, the Attorney General may elect to recover an award of statutory damages for each violation of subsection (b) in the sum of not less than $2,500 or more than $25,000.

(C) REPEATED VIOLATIONS.—In any case in which the Attorney General sustains the burden of proving, and the court finds, that a person has violated subsection (b) within 3 years after a final judgment was entered against the person for another such violation, the court may increase the award of damages up to triple the amount that would otherwise be awarded, as the court considers just.

(D) INNOCENT VIOLATIONS.—

(i) IN GENERAL.—The court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of

proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation.

(ii) NONPROFIT LIBRARY, ARCHIVE, EDUCATIONAL INSTITUTIONS, OR PUBLIC BROADCASTING ENTITIES.—In the case of a nonprofit library, archive, educational institution, or public broadcasting entity, the court shall remit damages in any case in which the library, archive, educational institution, or public broadcasting entity sustains the burden of proving, and the court finds, that the library, archive, educational institution, or public broadcasting entity was not aware and had no reason to believe that its acts constituted a violation.

SEC. 512. SENSE OF CONGRESS ON HOSTILE FOREIGN CYBER ACTORS.

It is the sense of Congress that foreign ransomware organizations, and foreign affiliates associated with them, constitute hostile foreign cyber actors, that covered nations abet and benefit from the activities of these actors, and that such actors should be treated as hostile foreign cyber actors by the United States. Such actors include the following:

(1) DarkSide.

(2) Conti.

(3) REvil.

(4) BlackCat, also known as "ALPHV".

(5) LockBit.

(6) Rhysida, also known as "Vice Society".

(7) Royal.

(8) Phobos, also known as "Eight" and also known as "Joanta".

(9) C10p.

(10) Hackers associated with the SamSam ransomware campaigns.

(11) Play.

(12) BianLian.

(13) Killnet.

(14) Akira.

(15) Ragnar Locker, also known as "Dark Angels".

(16) Blacksuit.

(17) INC.

(18) Black Basta.

SEC. 513. DESIGNATION OF STATE SPONSORS OF

RANSOMWARE AND REPORTING REQUIREMENTS.

(a) Designation of State Sponsors of Ransomware.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Secretary of State, in consultation with the Director of National Intelligence, shall—

(A) designate as a state sponsor of ransomware any country the government of which the Secretary has determined has provided support for ransomware demand schemes (including by providing safe haven for individuals engaged in such schemes);

(B) submit to Congress a report listing the countries designated under subparagraph (A); and

(C) in making designations under subparagraph (A), take into consideration the report submitted to Congress under section 514(c)(1).

(2) SANCTIONS AND PENALTIES.—The President shall impose with respect to each state sponsor of ransomware designated under paragraph (1)(A) the sanctions and penalties imposed with respect to a state sponsor of terrorism.

(3) STATE SPONSOR OF TERRORISM DEFINED.—In this subsection, the term "state sponsor of terrorism" means a country the government of which the Secretary of State has determined has repeatedly provided support for acts of international terrorism, for purposes of—

(A) section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (50 U.S.C. 4813(c)(1)(A)(i));

(B) section 620A of the Foreign Assistance Act of 1961 (22 U.S.C. 2371);

(C) section 40(d) of the Arms Export Control Act (22 U.S.C. 2780(d)); or

(D) any other provision of law.

(b) Reporting Requirements.—

(1) SANCTIONS RELATING TO RANSOMWARE REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of the Treasury shall submit a report to Congress that describes, for each of the 5 fiscal years immediately preceding the date of such report, the number and geographic locations of individuals, groups, and entities subject to sanctions imposed by the Office of Foreign Assets Control who were subsequently determined to have been involved in a ransomware demand scheme.

(2) COUNTRY OF ORIGIN REPORT.—The Secretary of State, in consultation with the Director of National Intelligence and the Director of the Federal Bureau of Investigation, shall—

(A) submit a report, with a classified annex, to the Committee on Foreign Relations of the Senate, the Select Committee on Intelligence of the Senate, the Committee on Foreign Affairs of the House of Representatives, and the Permanent Select Committee on Intelligence of the House of Representatives that identifies the country of origin of foreign-based ransomware attacks; and

(B) make the report described in subparagraph (A) (excluding the classified annex) available to the public.

(3) INVESTIGATIVE AUTHORITIES REPORT.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall issue a report that outlines the authorities available to the Federal Bureau of Investigation, the United States Secret Service, the Cybersecurity and Infrastructure Security Agency, Homeland Security Investigations, and the Office of Foreign Assets Control to respond to foreign-based ransomware attacks.

SEC. 514. DEEMING RANSOMWARE THREATS TO CRITICAL INFRASTRUCTURE A NATIONAL INTELLIGENCE PRIORITY.

(a) Critical Infrastructure Defined.—In this section, the term "critical infrastructure" has the meaning given such term in subsection (e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(b) Ransomware Threats to Critical Infrastructure as National Intelligence Priority.—The Director of National Intelligence, pursuant to the provisions of the National Security Act of 1947 (50 U.S.C. 3001 et seq.), the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), section 1.3(b)(17) of Executive Order 12333 (50 U.S.C. 3001 note; relating to United States intelligence activities), as in effect on the day before the date of the enactment of this Act, and National Security Presidential Directive–26 (February 24, 2003; relating to intelligence priorities), as in effect on the day before the date of the enactment of this Act, shall deem ransomware threats to critical infrastructure a national intelligence priority component to the National Intelligence Priorities Framework.

(c) Report.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in consultation with the Director of the Federal Bureau of Investigation, submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on the implications of the ransomware threat to United States national security.

(2) CONTENTS.—The report submitted under paragraph (1) shall address the following:

(A) Identification of individuals, groups, and entities who pose the most significant threat, including attribution to individual ransomware attacks whenever possible.

(B) Locations from which individuals, groups, and entities conduct ransomware attacks.

(C) The infrastructure, tactics, and techniques ransomware actors commonly use.

(D) Any relationships between the individuals, groups, and entities that conduct ransomware attacks and their governments or countries of origin that could impede the ability to counter ransomware threats.

(E) Intelligence gaps that have impeded, or currently are impeding, the ability to

counter ransomware threats.

(3) FORM.—The report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

TITLE VI—CLASSIFICATION REFORM

SEC. 601. GOVERNANCE OF CLASSIFICATION AND DECLASSIFICATION SYSTEM.

(a) Definitions.—In this section:

(1) CONTROLLED UNCLASSIFIED INFORMATION.—The term "controlled unclassified information" means information described as "Controlled Unclassified Information" or "CUI" in Executive Order 13556 (75 Fed. Reg. 68675; relating to controlled unclassified information), or any successor order.

(2) EXECUTIVE AGENT.—The term "Executive Agent" means the Executive Agent for Classification and Declassification designated under subsection (b)(1)(A).

(3) EXECUTIVE COMMITTEE.—The term "Executive Committee" means the Executive Committee on Classification and Declassification Programs and Technology established under subsection (b)(1)(C).

(b) Establishment of Classification and Declassification Governance.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President shall—

(A) designate a Federal official as Executive Agent for Classification and Declassification to identify and promote technological solutions to support efficient and effective systems for classification and declassification to be implemented on an interoperable and federated basis across the Federal Government;

(B) designate a Federal official—

(i) to establish policies and guidance relating to classification and declassification and controlled unclassified information across the Federal Government;

(ii) to conduct oversight of the implementation of such policies and guidance; and

(iii) who may, at the discretion of the President, also serve as Executive Agent; and

(C) establish an Executive Committee on Classification and Declassification Programs and Technology to provide direction, advice, and guidance to the Executive Agent.

(2) EXECUTIVE COMMITTEE.—

(A) COMPOSITION.—The Executive Committee shall be composed of the following or their designees:

(i) The Director of National Intelligence.

(ii) The Under Secretary of Defense for Intelligence and Security.

(iii) The Secretary of Energy.

(iv) The Secretary of State.

(v) The Director of the Office of Management and Budget.

(vi) The Archivist of the United States.

(vii) The Federal official designated under subsection (b)(1)(B) if such official is not also the Executive Agent.

(viii) Such other members as the Executive Agent considers appropriate.

(B) CHAIRPERSON.—The Executive Agent shall be the chairperson of the Executive Committee.

(c) Report to Congress.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President shall submit to Congress a report on the administration of this section.

(2) CONTENTS.—The report submitted pursuant to paragraph (1) shall include the following:

(A) Funding, personnel, expertise, and resources required for the Executive Agent and a description of how such funding, personnel, expertise, and resources will be provided.

(B) Authorities needed by the Executive Agent, a description of how such authorities will be granted, and a description of any additional statutory authorities required.

(C) Funding, personnel, expertise, and resources required by the Federal official designated under subsection (b)(1)(B) and a description of how such funding, personnel, expertise, and resources will be provided.

(D) Authorities needed by the Federal official designated under subsection (b)(1)(B), a description of how such authorities will be provided, and a description of any additional statutory authorities required.

(E) Funding and resources required by the Public Interest Declassification Board.

(d) Public Reporting.—

(1) IN GENERAL.—The report required by subsection (c) shall be made available to the public to the greatest extent possible consistent with the protection of sources and methods.

(2) PUBLICATION IN FEDERAL REGISTER.—The President shall publish in the Federal Register the roles and responsibilities of the Federal officials designated under subsection (b), the Executive Committee, and any subordinate individuals or entities.

SEC. 602. CLASSIFICATION AND DECLASSIFICATION

OF INFORMATION.

(a) In General.—Title VIII of the National Security Act of 1947 (50 U.S.C. 3161 et seq.) is amended by inserting after section 801 the following:

"SEC. 801A. CLASSIFICATION AND DECLASSIFICATION OF INFORMATION.

"(a) In General.—The President may, in accordance with this section, protect from unauthorized disclosure any information owned by, produced by or for, or under the control of the executive branch of the Federal Government when there is a demonstrable need to do so to protect the national security of the United States.

"(b) Establishment of Standards, Categories, and Procedures for Classification and Declassification.—

"(1) GOVERNMENTWIDE PROCEDURES.—

"(A) CLASSIFICATION.—The President shall, to the extent necessary, establish categories of information that may be classified and procedures for classifying information under subsection (a).

"(B) DECLASSIFICATION.—At the same time the President establishes categories and procedures under subparagraph (A), the President shall establish procedures for declassifying information that was previously classified.

"(C) MINIMUM REQUIREMENTS.—The procedures established pursuant to subparagraphs (A) and (B) shall—

"(i) be the exclusive means for classifying information on or after the effective date established by subsection (c), except with respect to information classified pursuant to the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.);

"(ii) ensure that no information is classified unless there is a demonstrable need to do so to protect the national security and there is a reasonable basis to believe that means other than classification will not provide sufficient protection;

"(iii) ensure that no information may remain classified indefinitely;

"(iv) ensure that no information shall be classified, continue to be maintained as classified, or fail to be declassified in order—

"(I) to conceal violations of law, inefficiency, or administrative error;

"(II) to prevent embarrassment to a person, organization, or agency;

"(III) to restrain competition; or

"(IV) to prevent or delay the release of information that does not require protection in the interest of the national security;

"(v) ensure that basic scientific research information not clearly related to the national security shall not be classified;

"(vi) ensure that information may not be reclassified after being declassified and released to the public under proper authority unless personally approved by the President based on a determination that such reclassification is required to prevent significant and demonstrable damage to the national security;

"(vii) establish standards and criteria for the classification of information;

"(viii) establish standards, criteria, and timelines for the declassification of information classified under this section;

"(ix) provide for the automatic declassification of classified records with permanent historical value not more than 50 years after the date of origin of such records, unless the head of each agency that classified information contained in such records makes a written determination to delay automatic declassification and such determination is reviewed not less frequently than every 10 years;

"(x) provide for the timely review of materials submitted for pre-publication;

"(xi) ensure that due regard is given for the public interest in disclosure of information;

"(xii) ensure that due regard is given for the interests of departments and agencies in sharing information at the lowest possible level of classification;

"(D) SUBMITTAL TO CONGRESS.—The President shall submit to Congress the categories and procedures established under subsection (b)(1)(A) and the procedures established under subsection (b)(1)(B) at least 60 days prior to their effective date.

"(2) AGENCY STANDARDS AND PROCEDURES.—

"(A) IN GENERAL.—The head of each agency shall establish a single set of consolidated standards and procedures to permit such agency to classify and declassify information created by such agency in accordance with the categories and procedures established by the President under this section and otherwise to carry out this section.

"(B) SUBMITTAL TO CONGRESS.—Each agency head shall submit to Congress the standards and procedures established by such agency head under subparagraph (A).

"(c) Effective Date.—

"(1) IN GENERAL.—Subsections (a) and (b) shall take effect on the date that is 180 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025.

"(2) RELATION TO PRESIDENTIAL DIRECTIVES.—Presidential directives regarding classifying, safeguarding, and declassifying national security information, including Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), in effect on the day before the date of the enactment of this Act, as well as procedures issued pursuant to such Presidential directives, shall remain in effect until superseded by procedures issued pursuant to subsection (b).".

(b) Conforming Amendment.—Section 805(2) of such Act (50 U.S.C. 3164(2)) is amended by inserting "section 801A," before "Executive Order".

(c) Clerical Amendment.—The table of contents preceding section 2 of such Act is amended

by inserting after the item relating to section 801 the following new item:

"Sec.801A.Classification and declassification of information.".

SEC. 603. MINIMUM STANDARDS FOR EXECUTIVE AGENCY INSIDER THREAT PROGRAMS.

(a) Definitions.—In this section:

(1) AGENCY.—The term "agency" means any Executive agency as defined in section 105 of title 5, United States Code, any military department as defined in section 102 of such title, and any other entity in the executive branch of the Federal Government that comes into the possession of classified information.

(2) CLASSIFIED INFORMATION.—The term "classified information" means information that has been determined to require protection from unauthorized disclosure pursuant to Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), or predecessor or successor order, to protect the national security of the United States.

(b) Establishment of Insider Threat Programs.—Each head of an agency with access to classified information shall establish an insider threat program to protect classified information from unauthorized disclosure.

(c) Minimum Standards.—In carrying out an insider threat program established by the head of an agency pursuant to subsection (b), the head of the agency shall—

(1) designate a senior official of the agency who shall be responsible for management of the program;

(2) monitor user activity on all classified networks to detect activity indicative of insider threat behavior;

(3) build and maintain an insider threat analytic and response capability to review, assess, and respond to information obtained pursuant to paragraph (2); and

(4) provide insider threat awareness training to all cleared employees within 30 days of entry-on-duty or granting of access to classified information and annually thereafter.

(d) Annual Reports.—Not less frequently than once each year, the Director of National Intelligence shall, serving as the Security Executive Agent under section 803 of the National Security Act of 1947 (50 U.S.C. 3162a), submit to Congress an annual report on the compliance of agencies with respect to the requirements of this section.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

SEC. 701. SECURITY CLEARANCES HELD BY CERTAIN FORMER EMPLOYEES OF INTELLIGENCE COMMUNITY.

(a) Issuance of Guidelines and Instructions Required.—Section 803(c) of the National Security Act of 1947 (50 U.S.C. 3162a(c)) is amended—

(1) in paragraph (3), by striking "; and" and inserting a semicolon;

(2) in paragraph (4), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(5) issue guidelines and instructions to the heads of Federal agencies to ensure that any individual who was appointed by the President to a position in an element of the intelligence community but is no longer employed by the Federal Government shall maintain a security clearance only in accordance with Executive Order 12968 (50 U.S.C. 3161 note; relating to access to classified information), or successor order.".

(b) Submittal of Guidelines and Instructions to Congress Required.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence shall, in the Director's capacity as the Security Executive Agent pursuant to subsection (a) of section 803 of the National Security Act of 1947 (50 U.S.C. 3162a), submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) the guidelines and instructions required by subsection (c)(5) of such Act, as added by subsection (a) of this section.

(c) Annual Report Required.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once each year thereafter, the Director of National Intelligence shall, in the Director's capacity as the Security Executive Agent pursuant to section 803(a) of the National Security Act of 1947 (50 U.S.C. 3162a(a)), submit to the congressional intelligence committees and the congressional defense committees (as defined in section 101(a) of title 10, United States Code) an annual report on the eligibility status of former senior employees of the intelligence community to access classified information.

(2) CONTENTS.—Each report submitted pursuant to paragraph (1) shall include, for the period covered by the report, the following:

(A) A list of individuals who were appointed by the President to a position in an element of the intelligence community who currently hold security clearances.

(B) The number of such former employees who still hold security clearances.

(C) For each former employee described in subparagraph (B)—

(i) the position in the intelligence community held by the former employee;

(ii) the years of service in such position; and

(iii) the individual's current employment position and employer.

(D) The Federal entity authorizing and adjudicating the former employees' need to know classified information.

SEC. 702. POLICY FOR AUTHORIZING INTELLIGENCE COMMUNITY PROGRAM OF CONTRACTOR-OWNED

AND CONTRACTOR-OPERATED SENSITIVE COMPARTMENTED INFORMATION FACILITIES.

(a) Policy.—The Director of National Intelligence shall establish a standardized policy for the intelligence community that authorizes a program of contractor-owned and contractor-operated sensitive compartmented information facilities as a service to the national security and intelligence enterprises.

(b) Requirements.—The policy established pursuant to subsection (a) shall—

(1) authorize the head of an element of the intelligence community to approve and accredit contractor-owned and contractor-operated sensitive compartmented information facilities; and

(2) designate an element of the intelligence community as a service of common concern (as defined in Intelligence Community Directive 122, or successor directive) to serve as an accrediting authority on behalf of other elements of the intelligence community for contractor-owned and contractor-operated sensitive compartmented information facilities.

(c) Cost Considerations.—In establishing the policy required by subsection (a), the Director shall consider existing demonstrated models where a contractor acquires, outfits, and manages a facility pursuant to an agreement with the Federal Government such that no funding from the Federal Government is required to carry out the agreement.

(d) Briefing Required.—Not later than 1 year after the date on which the Director establishes the policy pursuant to subsection (a), the Director shall brief the congressional intelligence committees on—

(1) additional opportunities to leverage contractor-provided secure facility space; and

(2) recommendations to address barriers, including resources or authorities needed.

SEC. 703. ENABLING INTELLIGENCE COMMUNITY INTEGRATION.

(a) In General.—The National Security Act of 1947 (50 U.S.C. 3001 et seq.) is amended by inserting after section 113B the following new section:

"SEC. 113C. ENABLING INTELLIGENCE COMMUNITY INTEGRATION.

"(a) Provision of Goods or Services.—Subject to and in accordance with any guidance and requirements developed by the Director of National Intelligence, the head of an element of the intelligence community may provide goods or services to another element of the intelligence community without reimbursement or transfer of funds for hoteling initiatives for intelligence community employees and affiliates defined in any such guidance and requirements issued by the Director of National Intelligence.

"(b) Approval.—Prior to the provision of goods or services pursuant to subsection (a), the head of the element of the intelligence community providing such goods or services and the head

of the element of the intelligence community receiving such goods or services shall approve such provision.".

(b) Clerical Amendment.—The table of contents of the National Security Act of 1947 is amended by inserting after the item relating to section 113B the following:

"Sec.113C.Enabling intelligence community integration.".

SEC. 704. APPOINTMENT OF SPOUSES OF CERTAIN FEDERAL EMPLOYEES.

(a) In General.—Section 3330d of title 5, United States Code, is amended—

(1) in the section heading, by striking "military and Department of Defense civilian spouses" and inserting "military and Department of Defense, Department of State, and intelligence community spouses";

(2) in subsection (a)—

(A) by redesignating the second paragraph (4) (relating to a spouse of an employee of the Department of Defense) as paragraph (7);

(B) by striking paragraph (5);

(C) by redesignating paragraph (4) (relating to the spouse of a disabled or deceased member of the Armed Forces) as paragraph (6);

(D) by striking paragraph (3) and inserting the following:

"(3) The term 'covered spouse' means an individual who is married to an individual who—

"(A)(i) is an employee of the Department of State or an element of the intelligence community; or

"(ii) is a member of the Armed Forces who is assigned to an element of the intelligence community; and

"(B) is transferred in the interest of the Government from one official station within the applicable agency to another within the agency (that is outside of normal commuting distance) for permanent duty.

"(4) The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

"(5) The term 'remote work' refers to a work flexibility arrangement under which an employee—

"(A) is not expected to physically report to the location from which the employee would otherwise work, considering the position of the employee; and

"(B) performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite—

"(i) other than the location from which the employee would otherwise work;

"(ii) that may be inside or outside the local commuting area of the location from which the employee would otherwise work; and

"(iii) that is typically the residence of the employee."; and

(E) by adding at the end the following:

"(8) The term 'telework' has the meaning given the term in section 6501."; and

(3) in subsection (b)—

(A) in paragraph (2), by striking "or" at the end;

(B) in the first paragraph (3) (relating to a spouse of a member of the Armed Forces on active duty), by striking the period at the end and inserting a semicolon;

(C) by redesignating the second paragraph (3) (relating to a spouse of an employee of the Department of Defense) as paragraph (4);

(D) in paragraph (4), as so redesignated—

(i) by inserting ", including to a position in which the spouse will engage in remote work" after "Department of Defense"; and

(ii) by striking the period at the end and inserting "; or"; and

(E) by adding at the end the following:

"(5) a covered spouse to a position in which the covered spouse will engage in remote work.".

(b) Technical and Conforming Amendment.—The table of sections for subchapter I of chapter 33 of title 5, United States Code, is amended by striking the item relating to section 3330d and inserting the following:

"3330d. Appointment of military and Department of Defense, Department of State, and intelligence community civilian spouses.".

SEC. 705. PLAN FOR STAFFING THE INTELLIGENCE COLLECTION POSITIONS OF THE CENTRAL INTELLIGENCE AGENCY.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Director of the Central Intelligence Agency shall submit to the congressional intelligence committees a plan for ensuring that the Directorate of Operations of the Agency has staffed every civilian full-time equivalent position authorized for that Directorate under the Intelligence Authorization Act for Fiscal Year 2024 (division G of Public Law 118–31).

(b) Elements.—The plan required by subsection (a) shall include the following:

(1) Specific benchmarks and timelines for accomplishing the goal described in such subsection by September 30, 2025.

(2) An assessment of the appropriate balance of staffing between the Directorate of Operations and the Directorate of Analysis consistent with the responsibilities of the

Director of the Central Intelligence Agency under section 104A(d) of the National Security Act of 1947 (50 U.S.C. 3036(d)).

SEC. 706. INTELLIGENCE COMMUNITY WORKPLACE PROTECTIONS.

(a) Employment Status.—

(1) CONVERSION OF POSITIONS BY DIRECTOR OF NATIONAL INTELLIGENCE TO EXCEPTED SERVICE.—Section 102A(v) of the National Security Act of 1947 (50 U.S.C. 3024(v)) is amended—

(A) by redesignating paragraphs (2) through (4) as paragraphs (3) through (5), respectively;

(B) by inserting after paragraph (1) the following:

"(2) The Director shall promptly notify the congressional intelligence committees of any action taken pursuant to paragraph (1)."; and

(C) in paragraph (3), as redesignated by subparagraph (A), by striking "occupying a position on the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2012".

(2) CONVERSION OF DEFENSE INTELLIGENCE POSITIONS TO EXCEPTED SERVICE.—Section 1601(a) of title 10, United States Code, is amended—

(A) by redesignating subsection (b) as subsection (d); and

(B) by inserting after subsection (a) the following:

"(b) Congressional Notification.—The Secretary shall promptly notify the congressional defense committees and the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) of any action taken pursuant to subsection (a).

"(c) Retention of Accrued Rights Upon Conversion.—An incumbent whose position is selected to be converted, without regard to the wishes of the incumbent, to the excepted service under subsection (a) shall remain in the competitive service for the purposes of status and any accrued adverse action protections while the individual occupies that position or any other position to which the employee is moved involuntarily. Once such individual no longer occupies the converted position, the position may be treated as a regularly excepted service position.".

(3) CONVERSION WITHIN THE EXCEPTED SERVICE.—An intelligence community incumbent employee whose position is selected to be converted from one excepted service schedule to another schedule within the excepted service without regard to the wishes of the incumbent shall remain in the current schedule for the purpose of status and any accrued adverse action protections while the individual occupies that position or any other position to which the employee is moved without regard to the wishes of the employee.

(b) Congressional Notification of Guidelines.—

(1) SUBMITTAL TO CONGRESS.—Not later than 30 days after the date of the enactment of this Act, each head of an element of the intelligence community shall submit to the

congressional intelligence committees the guidelines and regulations of the element relating to employment status and protections relating to that status.

(2) NOTICE OF CHANGES.—In any case in which a guideline or regulation of an element of the intelligence community submitted pursuant to paragraph (1) is modified or replaced, the head of the element shall promptly notify the congressional intelligence committees of the change and submit the new or modified guideline or regulation.

(c) Termination Authorities of the Director of the CIA.—

(1) PROCESS AND NOTIFICATION.—Section 104A(e) of the National Security Act of 1947 (50 U.S.C. 3036(e)) is amended—

(A) by redesignating paragraph (2) as paragraph (3); and

(B) by inserting after paragraph (1) the following:

"(2)(A) Subject to subparagraph (B), the Director shall not take an action under paragraph (1) to terminate the employment of an officer or employee, except in accordance with guidelines and regulations submitted to the congressional intelligence committees.

"(B) The Director may take an action under paragraph (1) without or in contravention of the guidelines and regulations specified in subparagraph (A) of this paragraph if the Director determines that complying with such guidelines and regulations poses a threat to the national security of the United States. If the Director makes such a determination, the Director shall provide prompt notification to the congressional intelligence committees that includes—

"(i) an explanation for the basis for the termination and the factual support for such determination; and

"(ii) an explanation for the determination that the process described in subparagraph (A) poses a threat to the national security of the United States.".

(d) Improvement of Congressional Notice Requirement Relating to Termination of Defense Intelligence Employees.—Section 1609(c) of title 10, United States Code, is amended by adding at the end the following: "Such notification shall include the following:

"(1) An explanation for the determination that the termination was in the interests of the United States.

"(2) An explanation for the determination that the procedures prescribed in other provisions of law that authorize the termination of the employment of such employee cannot be invoked in a manner consistent with the national security of the United States.".

(e) Congressional Notification of Other Suspension and Removal Authorities.—Section 7532 of title 5, United States Code, is amended by adding at the end the following:

"(d)(1) The head of an element of the intelligence community who takes an action under this section shall promptly notify the congressional intelligence committees of such action.

"(2) Each notification under paragraph (1) regarding an action shall include the following:

"(A) An explanation for the determination that the action is necessary or advisable in the interests of national security.

"(B) If the head of an element of the intelligence community determines, pursuant to subsection (a), that the interests of national security do not permit notification to the employee of the reasons for the action under that subsection, an explanation for such determination.

"(3) In this subsection, the terms 'congressional intelligence committees' and 'intelligence community' have the meanings given such terms in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).".

(f) Savings Clause.—Nothing in this section shall be construed to diminish the rights conferred by chapter 75 of title 5, United States Code, or other applicable agency adverse action or disciplinary procedures.

SEC. 707. SENSE OF CONGRESS ON GOVERNMENT PERSONNEL SUPPORT FOR FOREIGN TERRORIST ORGANIZATIONS.

It is the sense of Congress that for the purposes of adjudicating the eligibility of an individual for access to classified information, renewal of a prior determination of eligibility for such access, or continuous vetting of an individual for eligibility for such access, including on form SF–86 or any successor form, each of the following should be considered an action advocating for an act of terrorism:

(1) Espousing the actions of an organization designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(2) Advocating for continued attacks by an organization described in paragraph (1).

(3) Soliciting funds for an organization described in paragraph (1).

TITLE VIII—WHISTLEBLOWERS

SEC. 801. IMPROVEMENTS REGARDING URGENT CONCERNS SUBMITTED TO INSPECTORS GENERAL OF THE INTELLIGENCE COMMUNITY.

(a) Inspector General of the Intelligence Community.—Section 103H(k)(5) of the National Security Act of 1947 (50 U.S.C. 3033(k)(5)) is amended—

(1) in subparagraph (A)—

(A) by inserting "(i)" before "An employee of";

(B) by inserting "in writing" before "to the Inspector General"; and

(C) by adding at the end the following:

"(ii) The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this subparagraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.";

(2) by striking subparagraph (B) and inserting the following:

"(B)(i)(I) Not later than the end of the period specified in subclause (II), the Inspector General shall determine whether the written complaint or information submitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

"(II) The period specified in this subclause is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subparagraph (A) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subparagraph.

"(ii) The Inspector General may transmit a complaint or information submitted under subparagraph (A) directly to the congressional intelligence committees—

"(I) without transmittal to the Director if the Inspector General determines that transmittal to the Director could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(II) following transmittal to the Director if the Director does not transmit the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C).";

(3) in subparagraph (D)—

(A) in clause (i), by striking "or does not transmit the complaint or information to the Director in accurate form under subparagraph (B)," and inserting "does not transmit the complaint or information to the Director in accurate form under subparagraph (B)(i)(I), or makes a determination pursuant to subparagraph (B)(ii)(I) but does not transmit the complaint or information to the congressional intelligence committees within 21 calendar days of receipt,"; and

(B) by striking clause (ii) and inserting the following:

"(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if—

"(I) the employee, before making such a contact—

"(aa) transmits to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

"(bb) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices; or

"(II) the Inspector General—

"(aa) determines that—

"(AA) a transmittal under subclause (I) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(BB) the Director has failed to provide adequate direction pursuant to item (bb) of subclause (I) within 7 calendar days of a transmittal under such subclause; and

"(bb) provides the employee direction on how to contact the congressional intelligence committees in accordance with appropriate security practices."; and

(4) by adding at the end the following:

"(J) In this paragraph, the term 'employee', with respect to an employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community who may submit a complaint or information to the Inspector General under subparagraph (A), means—

"(i) a current employee at the time of such submission; or

"(ii) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.".

(b) Inspector General of the Central Intelligence Agency.—Section 17(d)(5) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(d)(5)) is amended—

(1) in subparagraph (A)—

(A) by inserting (i) before "An employee";

(B) by inserting "in writing" before "to the Inspector General"; and

(C) by adding at the end the following:

"(ii) The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this subparagraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.";

(2) in subparagraph (B)—

(A) by striking clause (i) and inserting the following:

"(i)(I) Not later than the end of the period specified in subclause (II), the Inspector General shall determine whether the written complaint or information submitted under subparagraph (A) appears credible. Upon making such a determination, the Inspector General shall transmit to the Director notice of that determination, together with the complaint or information.

"(II) The period specified in this subclause is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subparagraph (A) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subparagraph."; and

(B) by adding at the end the following:

"(iii) The Inspector General may transmit a complaint or information submitted under subparagraph (A) directly to the congressional intelligence committees—

"(I) without transmittal to the Director if the Inspector General determines that transmittal to the Director could compromise the anonymity of the employee or result in the complaint

or information being transmitted to a subject of the complaint or information;

"(II) following transmittal to the Director if the Director does not transmit the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C) and has not made a determination regarding a conflict of interest pursuant to clause (ii); or

"(III) following transmittal to the Director and a determination by the Director that a conflict of interest exists pursuant to clause (ii) if the Inspector General determines that—

"(aa) transmittal to the Director of National Intelligence could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(bb) the Director of National Intelligence has not transmitted the complaint or information to the congressional intelligence committees within the time period specified in subparagraph (C).";

(3) in subparagraph (D)—

(A) in clause (i), by striking "or does not transmit the complaint or information to the Director in accurate form under subparagraph (B)," and inserting "does not transmit the complaint or information to the Director in accurate form under subparagraph (B)(i)(I), or makes a determination pursuant to subparagraph (B)(iii)(I) but does not transmit the complaint or information to the congressional intelligence committees within 21 calendar days of receipt,"; and

(B) by striking clause (ii) and inserting the following:

"(ii) An employee may contact the congressional intelligence committees directly as described in clause (i) only if—

"(I) the employee, before making such a contact—

"(aa) transmits to the Director, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the congressional intelligence committees directly; and

"(bb) obtains and follows from the Director, through the Inspector General, direction on how to contact the congressional intelligence committees in accordance with appropriate security practices; or

"(II) the Inspector General—

"(aa) determines that—

"(AA) the transmittal under subclause (I) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(BB) the Director has failed to provide adequate direction pursuant to item (bb) of subclause (I) within 7 calendar days of a transmittal under such subclause; and

"(bb) provides the employee direction on how to contact the congressional

intelligence committees in accordance with appropriate security practices."; and

(4) by adding at the end the following:

"(I) In this paragraph, the term 'employee', with respect to an employee of the Agency, or of a contractor to the Agency, who may submit a complaint or information to the Inspector General under subparagraph (A), means—

"(i) a current employee at the time of such submission; or

"(ii) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.".

(c) Other Inspectors General of Elements of the Intelligence Community.—Section 416 of title 5, United States Code, is amended—

(1) in subsection (a)—

(A) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively; and

(B) by inserting before paragraph (2), as redesignated by paragraph (1), the following:

"(1) EMPLOYEE.—The term 'employee', with respect to an employee of an element of the Federal Government covered by subsection (b), or of a contractor to such an element, who may submit a complaint or information to an Inspector General under such subsection, means—

"(A) a current employee at the time of such submission; or

"(B) a former employee at the time of such submission, if such complaint or information arises from and relates to the period of employment as such an employee.";

(2) in subsection (b)—

(A) in paragraph (1)—

(i) in the paragraph heading, by inserting "; SUPPORT FOR WRITTEN SUBMISSION"; after "MADE";

(ii) by inserting "in writing" after "may report the complaint or information" each place it appears; and

(iii) in subparagraph (B), by inserting "in writing" after "such complaint or information"; and

(B) by adding at the end the following:

"(E) SUPPORT FOR WRITTEN SUBMISSION.—The Inspector General shall provide any support necessary to ensure that an employee can submit a complaint or information under this paragraph in writing and, if such submission is not feasible, shall create a written record of the employee's verbal complaint or information and treat such written record as a written submission.";

(3) in subsection (c)—

(A) by striking paragraph (1) and inserting the following:

"(1) CREDIBILITY.—

"(A) DETERMINATION.—Not later than the end of the period specified in subparagraph (B), the Inspector General shall determine whether the written complaint or information submitted under subsection (b) appears credible. Upon making such a determination, the Inspector General shall transmit to the head of the establishment notice of that determination, together with the complaint or information.

"(B) PERIOD SPECIFIED.—The period specified in this subparagraph is the 14-calendar-day period beginning on the date on which an employee who has submitted an initial written complaint or information under subsection (b) confirms that the employee has submitted to the Inspector General the material the employee intends to submit to Congress under such subsection."; and

(B) by adding at the end the following:

"(3) TRANSMITTAL DIRECTLY TO INTELLIGENCE COMMITTEES.—The Inspector General may transmit the complaint or information directly to the intelligence committees—

"(A) without transmittal to the head of the establishment if the Inspector General determines that transmittal to the head of the establishment could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information;

"(B) following transmittal to the head of the establishment if the head of the establishment does not transmit the complaint or information to the intelligence committees within the time period specified in subsection (d) and has not made a determination regarding a conflict of interest pursuant to paragraph (2); or

"(C) following transmittal to the head of the establishment and a determination by the head of the establishment that a conflict of interest exists pursuant to paragraph (2) if the Inspector General determines that—

"(i) transmittal to the Director of National Intelligence or the Secretary of Defense could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(ii) the Director of National Intelligence or the Secretary of Defense has not transmitted the complaint or information to the intelligence committees within the time period specified in subsection (d).";

(4) in subsection (e)(1), by striking "or does not transmit the complaint or information to the head of the establishment in accurate form under subsection (c)," and inserting "does not transmit the complaint or information to the head of the establishment in accurate form under subsection (c)(1)(A), or makes a determination pursuant to subsection (c)(3)(A) but does not transmit the complaint or information to the intelligence committees within 21 calendar days of receipt,"; and

(5) in subsection (e), by striking paragraph (2) and inserting the following:

"(2) LIMITATION.—An employee may contact the intelligence committees directly as described in paragraph (1) only if—

"(A) the employee, before making such a contact—

"(i) transmits to the head of the establishment, through the Inspector General, a statement of the employee's complaint or information and notice of the employee's intent to contact the intelligence committees directly; and

"(ii) obtains and follows from the head of the establishment, through the Inspector General, direction on how to contact the intelligence committees in accordance with appropriate security practices; or

"(B) the Inspector General—

"(i) determines that the transmittal under subparagraph (A) could compromise the anonymity of the employee or result in the complaint or information being transmitted to a subject of the complaint or information; or

"(ii) determines that the head of the establishment has failed to provide adequate direction pursuant to clause (ii) of subparagraph (A) within 7 calendar days of a transmittal under such subparagraph; and

"(iii) provides the employee direction on how to contact the intelligence committees in accordance with appropriate security practices.".

SEC. 802. PROHIBITION AGAINST DISCLOSURE OF WHISTLEBLOWER IDENTITY AS ACT OF REPRISAL.

(a) In General.—Section 1104(a) of the National Security Act of 1947 (50 U.S.C. 3234(a)) is amended—

(1) in paragraph (3)—

(A) in subparagraph (I), by striking "; or" and inserting a semicolon;

(B) by redesignating subparagraph (J) as subparagraph (K); and

(C) by inserting after subparagraph (I) the following:

"(J) an unauthorized whistleblower identity disclosure;"; and

(2) by adding at the end the following:

"(5) UNAUTHORIZED WHISTLEBLOWER IDENTITY DISCLOSURE.—The term 'unauthorized whistleblower identity disclosure' means, with respect to an employee or a contractor employee described in paragraph (3), a knowing and willful disclosure revealing the identity or other personally identifiable information of the employee or contractor employee so as to identify the employee or contractor employee as an employee or contractor employee who has made a lawful disclosure described in subsection (b) or (c), but does not include such a knowing and willful disclosure that meets any of the following criteria:

"(A) Such disclosure was made with the express consent of the employee or contractor employee.

"(B) Such disclosure was made during the course of reporting or remedying the subject of the lawful disclosure of the whistleblower through management, legal, or oversight processes, including such processes relating to human resources, equal opportunity, security, or an Inspector General.

"(C) An Inspector General with oversight responsibility for the relevant covered intelligence community element determines that such disclosure—

"(i) was unavoidable under section 103H of this Act (50 U.S.C. 3033), section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517), section 407 of title 5, United States Code, or section 420(b)(2)(B) of such title;

"(ii) was made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; or

"(iii) was required by statute or an order from a court of competent jurisdiction.".

(b) Private Right of Action for Unlawful Disclosure of Whistleblower Identity.—Subsection (f) of such section is amended to read as follows:

"(f) Enforcement.—

"(1) IN GENERAL.—Except as otherwise provided in this subsection, the President shall provide for the enforcement of this section.

"(2) HARMONIZATION WITH OTHER ENFORCEMENT.—To the fullest extent possible, the President shall provide for enforcement of this section in a manner that is consistent with the enforcement of section 2302(b)(8) of title 5, United States Code, especially with respect to policies and procedures used to adjudicate alleged violations of such section.

"(3) PRIVATE RIGHT OF ACTION FOR DISCLOSURES OF WHISTLEBLOWER IDENTITY IN VIOLATION OF PROHIBITION AGAINST REPRISALS.—Subject to paragraph (4), in a case in which an employee of an agency takes a personnel action described in subsection (a)(3)(J) against an employee of a covered intelligence community element as a reprisal in violation of subsection (b) or in a case in which an employee or contractor employee takes a personnel action described in subsection (a)(3)(J) against another contractor employee as a reprisal in violation of subsection (c), the employee or contractor employee against whom the personnel action was taken may, consistent with section 1221 of title 5, United States Code, bring a private action for all appropriate remedies, including injunctive relief and compensatory and punitive damages, in an amount not to exceed $250,000, against the agency of the employee or contracting agency of the contractor employee who took the personnel action, in a Federal district court of competent jurisdiction.

"(4) REQUIREMENTS.—

"(A) REVIEW BY INSPECTOR GENERAL AND BY EXTERNAL REVIEW PANEL.—Before the employee or contractor employee may bring a private action under paragraph (3), the employee or contractor employee shall exhaust administrative remedies by—

"(i) first, obtaining a disposition of their claim by requesting review by the appropriate inspector general; and

"(ii) second, if the review under clause (i) does not substantiate reprisal, by submitting to the Inspector General of the Intelligence Community a request for a review of the claim by an external review panel under section 1106.

"(B) PERIOD TO BRING ACTION.—The employee or contractor employee may bring a private right of action under paragraph (3) during the 180-day period beginning on the date on which the employee or contractor employee is notified of the final disposition of their claim under section 1106.".

SEC. 803. PROTECTION FOR INDIVIDUALS MAKING AUTHORIZED DISCLOSURES TO INSPECTORS GENERAL OF ELEMENTS OF THE INTELLIGENCE COMMUNITY.

(a) Inspector General of the Intelligence Community.—Section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 3033(g)(3)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(2) by adding at the end the following new subparagraph:

"(B) An individual may disclose classified information to the Inspector General in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or section 803, chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.), or any applicable provision of law. Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

"(i) any otherwise applicable nondisclosure agreement;

"(ii) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information) or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

"(iii) section 798 of title 18, United States Code, or any other provision of law relating to the unauthorized disclosure of national security information."; and

(3) in the paragraph enumerator, by striking "(3) " and inserting "(3)(A)".

(b) Inspector General of the Central Intelligence Agency.—Section 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3517(e)(3)) is amended—

(1) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively;

(2) by adding at the end the following new subparagraph:

"(B) An individual may disclose classified information to the Inspector General in accordance with the applicable security standards and procedures established under

Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or 803 of the National Security Act of 1947 (50 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

"(i) any otherwise applicable nondisclosure agreement;

"(ii) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

"(iii) section 798 of title 18, United States Code, or any other provision of law relating to the unauthorized disclosure of national security information."; and

(3) in the paragraph enumerator, by striking "(3) " and inserting "(3)(A)".

(c) Other Inspectors General of Elements of the Intelligence Community.—Section 416 of title 5, United States Code, is amended by adding at the end the following new subsection:

"(i) Protection for Individuals Making Authorized Disclosures.—An individual may disclose classified information to an Inspector General of an element of the intelligence community in accordance with the applicable security standards and procedures established under Executive Order 13526 (50 U.S.C. 3161 note; relating to classified national security information), section 102A or 803 of the National Security Act of 1947 (50 U.S.C. 3024; 3162a), or chapter 12 of the Atomic Energy Act of 1954 (42 U.S.C. 2161 et seq.). Such a disclosure of classified information that is made by an individual who at the time of the disclosure does not hold the appropriate clearance or authority to access such classified information, but that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure and does not violate—

"(1) any otherwise applicable nondisclosure agreement;

"(2) any otherwise applicable regulation or order issued under the authority of Executive Order 13526 or chapter 18 of the Atomic Energy Act of 1954 (42 U.S.C. 2271 et seq.); or

"(3) section 798 of title 18, or any other provision of law relating to the unauthorized disclosure of national security information.".

SEC. 804. CLARIFICATION OF AUTHORITY OF CERTAIN INSPECTORS GENERAL TO RECEIVE PROTECTED DISCLOSURES.

Section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) is amended—

(1) in subsection (b)(1), by inserting "or covered intelligence community element" after "the appropriate inspector general of the employing agency"; and

(2) in subsection (c)(1)(A), by inserting "or covered intelligence community element" after "the appropriate inspector general of the employing or contracting agency".

SEC. 805. WHISTLEBLOWER PROTECTIONS RELATING TO PSYCHIATRIC TESTING OR EXAMINATION.

(a) Prohibited Personnel Practices.—Section 1104(a)(3) of the National Security Act of 1947 (50 U.S.C. 3234(a)(3)) is amended—

(1) in subparagraph (I), by striking "; or" and inserting a semicolon;

(2) by redesignating subparagraph (J) as subparagraph (K); and

(3) by inserting after subparagraph (I) the following new subparagraph:

"(J) a decision to order psychiatric testing or examination; or".

(b) Application.—The amendments made by this section shall apply with respect to matters arising under section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) on or after the date of the enactment of this Act.

SEC. 806. ESTABLISHING PROCESS PARITY FOR ADVERSE SECURITY CLEARANCE AND ACCESS DETERMINATIONS.

Subparagraph (C) of section 3001(j)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(4)) is amended to read as follows:

"(C) CONTRIBUTING FACTOR.—

"(i) IN GENERAL.—Subject to clause (iii), in determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall find that paragraph (1) was violated if the individual has demonstrated that a disclosure described in paragraph (1) was a contributing factor in the adverse security clearance or access determination taken against the individual.

"(ii) CIRCUMSTANTIAL EVIDENCE.—An individual under clause (i) may demonstrate that the disclosure was a contributing factor in the adverse security clearance or access determination taken against the individual through circumstantial evidence, such as evidence that—

"(I) the official making the determination knew of the disclosure; and

"(II) the determination occurred within a period such that a reasonable person could conclude that the disclosure was a contributing factor in the determination.

"(iii) DEFENSE.—In determining whether the adverse security clearance or access determination violated paragraph (1), the agency shall not find that paragraph (1) was violated if, after a finding that a disclosure was a contributing factor, the agency demonstrates by clear and convincing evidence that it would have made the same security clearance or access determination in the absence of such disclosure.".

SEC. 807. ELIMINATION OF CAP ON COMPENSATORY DAMAGES FOR RETALIATORY REVOCATION OF SECURITY CLEARANCES AND ACCESS DETERMINATIONS.

Section 3001(j)(4)(B) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(j)(4)(B)) is amended, in the second sentence, by striking "not to exceed $300,000".

TITLE IX—ANOMALOUS HEALTH INCIDENTS

SEC. 901. ADDITIONAL DISCRETION FOR DIRECTOR OF CENTRAL INTELLIGENCE AGENCY IN PAYING COSTS OF TREATING QUALIFYING INJURIES AND MAKING PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.

(a) Additional Authority for Covering Costs for Treating Qualifying Injuries Under Extraordinary Circumstances.—Subsection (c) of section 19A of the Central Intelligence Agency Act of 1949 (50 U.S.C. 3519b) is amended—

(1) by striking "The Director may" and inserting the following:

"(1) IN GENERAL.—The Director may"; and

(2) by adding at the end the following:

"(2) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Director determines extraordinary, the Director may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by a provision of Federal law, regardless of the date of the injury and the location of the employee, individual, or dependent when the injury occurred.".

(b) Additional Authority for Making Payments for Qualifying Injuries to the Brain Under Extraordinary Circumstances.—Subsection (d)(2) of such section is amended—

(1) by striking "Notwithstanding" and inserting the following:

"(A) IN GENERAL.—Notwithstanding"; and

(2) by adding at the end the following:

"(B) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Director determines extraordinary, the Director may provide payment to a covered employee, a covered individual, or a covered dependent for any qualifying injury to the brain, regardless of the date of the injury and the location of the employee, individual, or dependent when the injury occurred.".

(c) Congressional Notification.—Such section is amended by adding at the end the following new subsection:

"(e) Congressional Notification.—Whenever the Director makes a payment or reimbursement made under subsection (c) or (d)(2), the Director shall, not later than 30 days after the date on which the payment or reimbursement is made, submit to the congressional intelligence committees (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) a notification of such payment or reimbursement.".

SEC. 902. ADDITIONAL DISCRETION FOR SECRETARY OF STATE AND HEADS OF OTHER FEDERAL AGENCIES IN PAYING COSTS OF TREATING QUALIFYING INJURIES AND MAKING PAYMENTS FOR QUALIFYING INJURIES TO THE BRAIN.

(a) Additional Authority for Covering Costs for Treating Qualifying Injuries Under Extraordinary Circumstances.—Subsection (b) of section 901 of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b) is amended to read as follows:

"(b) Costs for Treating Qualifying Injuries.—

"(1) IN GENERAL.—The Secretary of State or the head of any other Federal agency may pay or reimburse the costs relating to diagnosing and treating—

"(A) a qualifying injury of a covered employee for such costs, that are not otherwise covered by chapter 81 of title 5, United States Code, or other provision of Federal law; or

"(B) a qualifying injury of a covered individual, or a covered dependent, for such costs that are not otherwise covered by Federal law.

"(2) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Secretary of State or other agency head determines extraordinary, the Secretary or other agency head may pay the costs of treating a qualifying injury of a covered employee, a covered individual, or a covered dependent or may reimburse a covered employee, a covered individual, or a covered dependent for such costs, that are not otherwise covered by a provision of Federal law, regardless of the date on which the injury occurred.".

(b) Additional Authority for Making Payments for Qualifying Injuries to the Brain Under Extraordinary Circumstances.—Subsection (i)(2) of such section is amended—

(1) by striking "Notwithstanding" and inserting the following:

"(A) IN GENERAL.—Notwithstanding"; and

(2) by adding at the end the following:

"(B) EXTRAORDINARY CIRCUMSTANCES.—Under such circumstances as the Secretary of State or other agency head with an employee determines extraordinary, the Secretary or other agency head may provide payment to a covered dependent, a dependent of a former employee, a covered employee, a former employee, and a covered individual for any qualifying injury to the brain, regardless of the date on which the injury occurred.".

(c) Changes to Definitions.—Subsection (e) of such section is amended—

(1) in paragraph (1)—

(A) in the matter before subparagraph (A), by striking "a employee who, on or after January 1, 2016" and inserting "an employee who, on or after September 11, 2001"; and

(B) in subparagraph (A), by inserting ", or duty station in the United States" before the semicolon;

(2) in paragraph (2)—

(A) by striking "January 1, 2016" and inserting "September 11, 2001"; and

(B) by inserting ", or duty station in the United States," after "pursuant to subsection (f)";

(3) in paragraph (3)—

(A) in the matter before subparagraph (A), by striking "January 1, 2016" and inserting "September 11, 2001"; and

(B) in subparagraph (A), by inserting ", or duty station in the United States" before the semicolon; and

(4) in paragraph (4)—

(A) in subparagraph (A)(i), by inserting ", or duty station in the United States" before the semicolon; and

(B) in subparagraph (B)(i), by inserting ", or duty station in the United States" before the semicolon.

(d) Clarification Relating to Authorities of Director of the Central Intelligence Agency.—Such section is further amended by adding at the end the following:

"(k) Relation to Director of Central Intelligence Agency.—The authorities and requirements of this section shall not apply to the Director of the Central Intelligence Agency.".

SEC. 903. IMPROVED FUNDING FLEXIBILITY FOR PAYMENTS MADE BY DEPARTMENT OF STATE FOR QUALIFYING INJURIES TO THE BRAIN.

Section 901(i) of division J of the Further Consolidated Appropriations Act, 2020 (22 U.S.C. 2680b) is amended by striking paragraph (3) and inserting the following:

"(3) FUNDING.—

"(A) IN GENERAL.—Payment under paragraph (2) in a fiscal year may be made using any funds—

"(i) appropriated specifically for payments under such paragraph; or

"(ii) reprogrammed in accordance with an applicable provision of law.

"(B) BUDGET.—For each fiscal year, the Secretary of State shall include with the budget justification materials submitted to Congress in support of the budget of the President for that fiscal year pursuant to section 1105(a) of title 31, United States Code, an estimate of the funds required in that fiscal year to make payments under paragraph (2).".

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

SEC. 1001. COMPTROLLER GENERAL OF THE UNITED STATES REVIEW OF ALL-DOMAIN ANOMALY RESOLUTION OFFICE.

(a) Definitions.—In this section, the terms "congressional defense committees", "congressional leadership", and "unidentified anomalous phenomena" have the meanings given such terms in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)).

(b) Review Required.—The Comptroller General of the United States shall conduct a review of the All-domain Anomaly Resolution Office (in this section referred to as the "Office").

(c) Elements.—The review conducted pursuant to subsection (b) shall include the following:

(1) A review of the implementation by the Office of the duties and requirements of the Office under section 1683 of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373), such as the process for operational unidentified anomalous phenomena reporting and coordination with the Department of Defense, the intelligence community, and other departments and agencies of the Federal Government and non-Government entities.

(2) A review of such other matters relating to the activities of the Office that pertain to unidentified anomalous phenomena as the Comptroller General considers appropriate.

(d) Report.—Following the review required by subsection (b), in a timeframe mutually agreed upon by the congressional intelligence committees, the congressional defense committees, congressional leadership, and the Comptroller General, the Comptroller General shall submit to such committees and congressional leadership a report on the findings of the Comptroller General with respect to the review conducted under subsection (b).

SEC. 1002. SUNSET OF REQUIREMENTS RELATING TO AUDITS OF UNIDENTIFIED ANOMALOUS PHENOMENA HISTORICAL RECORD REPORT.

Section 6001 of the Intelligence Authorization Act for Fiscal Year 2023 (50 U.S.C. 3373 note) is amended—

(1) in subsection (b)(2), by inserting "until April 1, 2025" after "quarterly basis"; and

(2) in subsection (c), by inserting "until June 30, 2025" after "semiannually thereafter".

SEC. 1003. FUNDING LIMITATIONS RELATING TO UNIDENTIFIED ANOMALOUS PHENOMENA.

(a) Definitions.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term "appropriate committees of Congress" means—

(A) the Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Appropriations of the Senate; and

(B) the Permanent Select Committee on Intelligence, the Committee on Armed Services, and the Committee on Appropriations of the House of Representatives.

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" means—

(A) the majority leader of the Senate;

(B) the minority leader of the Senate;

(C) the Speaker of the House of Representatives; and

(D) the minority leader of the House of Representatives.

(3) UNIDENTIFIED ANOMALOUS PHENOMENA.—The term "unidentified anomalous phenomena" has the meaning given such term in section 1683(n) of the National Defense Authorization Act for Fiscal Year 2022 (50 U.S.C. 3373(n)).

(b) Limitations.—None of the funds authorized to be appropriated or otherwise made available by this Act may be obligated or expended in support of any activity involving unidentified anomalous phenomena protected under any form of special access or restricted access limitation unless the Director of National Intelligence has provided the details of the activity to the appropriate committees of Congress and congressional leadership, including for any activities described in a report released by the All-domain Anomaly Resolution Office in fiscal year 2024.

(c) Limitation Regarding Independent Research and Development.—Independent research and development funding relating to unidentified anomalous phenomena shall not be allowable as indirect expenses for purposes of contracts covered by such instruction, unless such material and information is made available to the appropriate congressional committees and leadership.

TITLE XI—AIR AMERICA

SEC. 1101. SHORT TITLE.

This title may be cited as the "Air America Act of 2024".

SEC. 1102. FINDINGS.

Congress finds the following:

(1) Air America and its affiliated companies, in coordination with the Central Intelligence Agency, provided direct and indirect support to the United States Government from 1950 to 1976.

(2) The service and sacrifice of employees of Air America included—

(A) suffering a high rate of casualties in the course of service;

(B) saving thousands of lives in search and rescue missions for downed United States airmen and in allied refugee evacuations; and

(C) serving lengthy periods under challenging circumstances abroad.

SEC. 1103. DEFINITIONS.

In this title:

(1) AFFILIATED COMPANY.—The term "affiliated company", with respect to Air America, includes Air Asia Company Limited, CAT Incorporated, Civil Air Transport Company Limited, and the Pacific Division of Southern Air Transport.

(2) AIR AMERICA.—The term "Air America" means Air America, Incorporated.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(B) the Committee on Oversight and Accountability, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(4) CHILD; DEPENDENT; WIDOW; WIDOWER.—The terms "child", "dependent", "widow", and "widower" have the meanings given those terms in section 8341(a) of title 5, United States Code, except that such section shall be applied by substituting "individual who performed qualifying service" for "employee or Member".

(5) COVERED DECEDENT.—The term "covered decedent" means an individual who was killed in Southeast Asia while supporting operations of the Central Intelligence Agency during the period beginning on January 1, 1950, and ending on December 31, 1976, as a United States citizen employee of Air America or an affiliated company.

(6) DIRECTOR.—The term "Director" means the Director of the Central Intelligence Agency.

(7) QUALIFYING SERVICE.— The term "qualifying service" means service that—

(A) was performed by a United States citizen as an employee of Air America or an affiliated company during the period beginning on January 1, 1950, and ending on December 31, 1976; and

(B) is documented in—

(i) the corporate records of Air America or an affiliated company;

(ii) records possessed by the United States Government; or

(iii) the personal records of a former employee of Air America or an affiliated company that are verified by the United States Government.

(8) SURVIVOR.—The term "survivor" means—

(A) the widow or widower of—

(i) an individual who performed qualifying service; or

(ii) a covered decedent; or

(B) an individual who, at any time during or since the period of qualifying service, or on the date of death of a covered decedent, was a dependent or child of—

(i) the individual who performed such qualifying service; or

(ii) the covered decedent.

SEC. 1104. AWARD AUTHORIZED TO ELIGIBLE PERSONS.

(a) In General.—Subject to the limitation in subsection (d), the Director shall provide an award payment of $40,000 under this section—

(1) to an individual who performed qualifying service for a period greater than or equal to 5 years or to a survivor of such individual; or

(2) to the survivor of a covered decedent.

(b) Requirements.—

(1) IN GENERAL.—To be eligible for a payment under this subsection, an individual who performed qualifying service or survivor (as the case may be) must demonstrate to the satisfaction of the Director that the individual whose qualifying service upon which the payment is based meets the criteria of paragraph (1) or (2) of subsection (a).

(2) RELIANCE ON RECORDS.—In carrying out this subsection, in addition to any evidence provided by such an individual or survivor, the Director may rely on records possessed by the United States Government.

(c) Additional Payment.—If an individual, or in the case of a survivor, the individual whose qualifying service upon which the payment is based, can demonstrate to the Director that the qualifying service of the individual exceeded 5 years, the Director shall pay to such individual or survivor an additional $8,000 for each full year in excess of 5 years (and a proportionate amount for a partial year).

(d) Survivors.—In the case of an award granted to a survivor under this section, the payment shall be made—

(1) to the surviving widow or widower; or

(2) if there is no surviving widow or widower, to the surviving dependents or children, in equal shares.

SEC. 1105. FUNDING LIMITATION.

(a) In General.—The total amount of awards granted under this title may not exceed $60,000,000.

(b) Requests for Additional Funds.—If, at the determination of the Director, the amount of funds required to satisfy all valid applications for payment under this title exceeds the limitation set forth in subsection (a), the Director shall submit to Congress a request for sufficient funds to fulfill all remaining payments.

(c) Awards to Employees of Intermountain Aviation.—The Director may determine, on a case-by-case basis, to award amounts to individuals who performed service consistent with the definition of qualifying service as employees of Intermountain Aviation.

SEC. 1106. TIME LIMITATION.

(a) In General.—To be eligible for an award payment under this title, a claimant must file a claim for such payment with the Director not later than 2 years after the effective date of the regulations prescribed by the Director in accordance with section 1107.

(b) Determination.—Not later than 90 days after receiving a claim for an award payment under this section, the Director shall determine the eligibility of the claimant for payment.

(c) Payment.—

(1) IN GENERAL.—If the Director determines that the claimant is eligible for the award payment, the Director shall pay the award payment not later than 60 days after the date of such determination.

(2) LUMP-SUM PAYMENT.—The Director shall issue each payment as a one-time lump sum payment contingent upon the timely filing of the claimant under this section.

(3) NOTICE AND DELAYS.—The Director shall notify the appropriate congressional committees of any delays in making an award payment not later than 30 days after the date such payment is due.

SEC. 1107. APPLICATION PROCEDURES.

(a) In General.—The Director shall prescribe procedures to carry out this title, which shall include processes under which—

(1) claimants may submit claims for payment under this title;

(2) the Director will award the amounts under section 1104; and

(3) claimants can obtain redress and appeal determinations under section 1106.

(b) Other Matters.—Such procedures—

(1) shall be—

(A) prescribed not later than 60 days after the date of the enactment of this Act; and

(B) published in the Code of Federal Regulations; and

(2) shall not be subject to chapter 5 of title 5, United States Code.

SEC. 1108. RULE OF CONSTRUCTION.

Nothing in this title shall be construed to—

(1) entitle any person to Federal benefits, including retirement benefits under chapter 83 or 84 of title 5, United States Code, and disability or death benefits under chapter 81 of such title;

(2) change the legal status of the former Air America corporation or any affiliated company; or

(3) create any legal rights, benefits, or entitlements beyond the one-time award authorized by this title.

SEC. 1109. ATTORNEYS' AND AGENTS' FEES.

(a) In General.—It shall be unlawful for more than 25 percent of an award paid pursuant to this title to be paid to, or received by, any agent or attorney for any service rendered to a person who receives an award under section 1104, in connection with the award under this title.

(b) Violation.—Any agent or attorney who violates subsection (a) shall be fined under title 18, United States Code.

SEC. 1110. NO JUDICIAL REVIEW.

A determination by the Director pursuant to this title is final and conclusive and shall not be subject to judicial review.

SEC. 1111. REPORTS TO CONGRESS.

Until the date that all funds available for awards under this title are expended, the Director shall submit to the appropriate congressional committees a semiannual report describing the number of award payments made and denied during the 180 days preceding the submission of the report, including the rationales for any denials, and if, at the determination of the Director, the amount of funds provided to carry out this title is insufficient to satisfy any remaining or anticipated claims.

TITLE XII—OTHER MATTERS

SEC. 1201. ENHANCED AUTHORITIES FOR AMICUS CURIAE UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) Expansion of Appointment Authority.—

(1) IN GENERAL.—Section 103(i)(2)(A) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(i)(2)(A)) is amended by striking clause (i) and inserting the following:

"(i) shall appoint one or more individuals who have been designated under paragraph (1), not less than one of whom possesses privacy and civil liberties expertise, unless the court finds that such a qualification is inappropriate, to serve as amicus curiae to assist the court in the consideration of any application or motion for an order or review that, in the opinion of the court—

"(I) presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate;

"(II) presents exceptional concerns with respect to the activities of a United States person that are protected by the first amendment to the Constitution of the United States, unless the court issues a finding that such appointment is not appropriate;

"(III) targets a United States person and presents or involves a sensitive investigative matter, unless—

"(aa) the matter represents an immediate danger to human life; or

"(bb) the court issues a finding that such appointment is not appropriate;

"(IV) targets a United States person and presents a request for approval of programmatic surveillance or reauthorization of programmatic surveillance, unless the court issues a finding that such appointment is not appropriate; or

"(V) targets a United States person and otherwise presents novel or exceptional civil liberties issues, unless the court issues a finding that such appointment is not appropriate;".

(2) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—Subsection (i) of section 103 of such Act (50 U.S.C. 1803) is amended by adding at the end the following:

"(12) DEFINITION OF SENSITIVE INVESTIGATIVE MATTER.—In this subsection, the term 'sensitive investigative matter' means—

"(A) an investigative matter that targets a United States person who is—

"(i) a United States elected official;

"(ii) an appointee of—

"(I) the President; or

"(II) a State Governor;

"(iii) a United States political candidate;

"(iv) a United States political organization or an individual prominent in such an organization;

"(v) a United States news media organization or a member of a United States news media organization; or

"(vi) a United States religious organization or an individual prominent in such an organization; or

"(B) any other investigative matter involving a domestic entity or a known or presumed United States person that, in the judgment of the applicable court established under subsection (a) or (b), is as sensitive as an investigative matter described in subparagraph (A).".

(b) Authority To Seek Review.—Subsection (i) of such section (50 U.S.C. 1803), as amended

by subsection (a) of this section, is further amended—

(1) in paragraph (4)—

(A) in the paragraph heading, by inserting "; AUTHORITY" after "DUTIES";

(B) by striking "the amicus curiae shall" and all that follows through "provide" and insert the following: "the amicus curiae—

"(A) shall provide";

(C) in subparagraph (A), as so designated—

(i) in clause (i), by inserting before the semicolon at the end the following: ", including legal arguments regarding any privacy or civil liberties interest of any United States person that would be significantly impacted by the application or motion"; and

(ii) in clause (iii), by striking the period at the end and inserting "; and"; and

(D) by adding at the end the following:

"(B) may seek leave to raise any novel or significant privacy or civil liberties issue relevant to the application or motion or other issue directly impacting the legality of the proposed electronic surveillance with the court, regardless of whether the court has requested assistance on that issue.";

(2) by redesignating paragraphs (7) through (12) as paragraphs (8) through (13), respectively; and

(3) by inserting after paragraph (6) the following:

"(7) AUTHORITY TO SEEK REVIEW OF DECISIONS.—

"(A) FISA COURT DECISIONS.—Following issuance of a final order under this Act by the Foreign Intelligence Surveillance Court in a matter in which an amicus curiae was appointed under paragraph (2), that amicus curiae may petition the Foreign Intelligence Surveillance Court to certify for review to the Foreign Intelligence Surveillance Court of Review a question of law pursuant to subsection (j). If the court denies such petition, the court shall provide for the record a written statement of the reasons for such denial. Upon certification of any question of law pursuant to this subparagraph, the Court of Review shall appoint the amicus curiae to assist the Court of Review in its consideration of the certified question, unless the Court of Review issues a finding that such appointment is not appropriate.

"(B) FISA COURT OF REVIEW DECISIONS.—An amicus curiae appointed under paragraph (2) may petition the Foreign Intelligence Surveillance Court of Review to certify for review to the Supreme Court of the United States any question of law pursuant to section 1254(2) of title 28, United States Code, in the matter in which that amicus curiae was appointed.

"(C) DECLASSIFICATION OF REFERRALS.—For purposes of section 602, if the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review denies a petition filed under subparagraph (A) or (B) of this paragraph, that

petition and all of its content shall be considered a decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review described in section 602(a).".

(c) Access to Information.—

(1) APPLICATION AND MATERIALS.—Subparagraph (A) of section 103(i)(6) of such Act (50 U.S.C. 1803(i)(6)) is amended to read as follows:

"(A) IN GENERAL.—

"(i) RIGHTS OF AMICUS.—If a court established under subsection (a) or (b) appoints an amicus curiae under paragraph (2), the amicus curiae—

"(I) shall have access to, to the extent such information is available to the Government and the court established under subsection (a) or (b) determines it is necessary to fulfill the duties of the amicus curiae—

"(aa) the application, certification, petition, motion, and other information and supporting materials submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed, including access to any relevant legal precedent (including any such precedent that is cited by the Government, including in such an application);

"(bb) a copy of each relevant decision made by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review in which the court decides a question of law, without regard to whether the decision is classified; and

"(cc) any other information or materials that the court determines are relevant to the duties of the amicus curiae; and

"(II) may make a submission to the court requesting access to any other particular materials or information (or category of materials or information) that the amicus curiae believes to be relevant to the duties of the amicus curiae.

"(ii) SUPPORTING DOCUMENTATION REGARDING ACCURACY.—The Foreign Intelligence Surveillance Court, upon the motion of an amicus curiae appointed under paragraph (2) or upon its own motion, may require the Government to make available the supporting documentation regarding the accuracy of any material submitted to the Foreign Intelligence Surveillance Court in connection with the matter in which the amicus curiae has been appointed if the court determines the information is relevant to the duties of the amicus curiae.".

(2) CLARIFICATION OF ACCESS TO CERTAIN INFORMATION.—Such section is further amended by striking subparagraph (C) and inserting the following:

"(C) CLASSIFIED INFORMATION.—An amicus curiae appointed by the court shall have access, to the extent such information is available to the Government and the court determines such information is relevant to the duties of the amicus curiae in the matter in which the amicus curiae was appointed, to copies of each opinion, order,

transcript, pleading, or other document of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review, including, if the individual is eligible for access to classified information, any classified documents, information, and other materials or proceedings, but only to the extent consistent with the national security of the United States.".

(3) CONSULTATION AMONG AMICI CURIAE.—Such section is further amended—

(A) by redesignating subparagraphs (B), (C), and (D) as subparagraphs (C), (D), and (E), respectively; and

(B) by inserting after subparagraph (A) the following:

"(B) CONSULTATION.—If the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review determines that it is relevant to the duties of an amicus curiae appointed by the court under paragraph (2), the amicus curiae may consult with one or more of the other individuals designated to serve as amicus curiae pursuant to paragraph (1) regarding any of the information relevant to any assigned proceeding.".

(d) Term Limits.—

(1) REQUIREMENT.—Paragraph (1) of section 103(i) of such Act (50 U.S.C. 1803(i)) is amended by adding at the end the following new sentence: "An individual may serve as an amicus curiae for a 5-year term, and the presiding judges may, for good cause, jointly reappoint the individual to a single additional 5-year term.".

(2) APPLICATION.—The amendment made by paragraph (1) shall apply with respect to the service of an amicus curiae appointed under section 103(i) of such Act (50 U.S.C. 1803(i)) that occurs on or after the date of the enactment of this Act, regardless of the date on which the amicus curiae is appointed.

SEC. 1202. LIMITATION ON DIRECTIVES UNDER FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 RELATING TO CERTAIN ELECTRONIC COMMUNICATION SERVICE PROVIDERS.

Section 702(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1881a(i)) is amended by adding at the end the following:

"(7) LIMITATION RELATING TO CERTAIN ELECTRONIC COMMUNICATION SERVICE PROVIDERS.—

"(A) DEFINITIONS.—In this paragraph:

"(i) APPROPRIATE COMMITTEES OF CONGRESS.—The term 'appropriate committees of Congress' means—

"(I) the congressional intelligence committees;

"(II) the Committee on the Judiciary of the Senate; and

"(III) the Committee on the Judiciary of the House of Representatives.

"(ii) COVERED ELECTRONIC COMMUNICATION SERVICE PROVIDER.—The term 'covered electronic communication service provider' means—

"(I) a service provider described in section 701(b)(4)(E); or

"(II) a custodian of an entity as defined in section 701(b)(4)(F).

"(iii) COVERED OPINIONS.—The term 'covered opinions' means the opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review authorized for public release on August 23, 2023 (Opinion and Order, In re Petition to Set Aside or Modify Directive Issued to [REDACTED], No. [REDACTED], (FISA Ct. [REDACTED] 2022) (Contreras J.); Opinion, In re Petition to Set Aside or Modify Directive Issued to [REDACTED], No. [REDACTED], (FISA Ct. Rev. [REDACTED] 2023) (Sentelle, J.; Higginson, J.; Miller J.)).

"(B) LIMITATION.—A directive may not be issued under paragraph (1) to a covered electronic communication service provider unless the covered electronic communication service provider is a provider of the type of service at issue in the covered opinions.

"(C) REQUIREMENTS FOR DIRECTIVES TO COVERED ELECTRONIC COMMUNICATION SERVICE PROVIDERS.—

"(i) IN GENERAL.—Subject to clause (ii), any directive issued under paragraph (1) on or after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 to a covered electronic communication service provider that is not prohibited by subparagraph (B) of this paragraph shall include a summary description of the services at issue in the covered opinions.

"(ii) DUPLICATE SUMMARIES NOT REQUIRED.—A directive need not include a summary description of the services at issue in the covered opinions if such summary was included in a prior directive issued to the covered electronic communication service provider and the summary has not materially changed.

"(D) FOREIGN INTELLIGENCE SURVEILLANCE COURT NOTIFICATION AND REVIEW.—

"(i) NOTIFICATION.—

"(I) IN GENERAL.—Subject to subclause (II), each time the Attorney General and the Director of National Intelligence issue a directive under paragraph (1) to a covered electronic communication service provider that is not prohibited by subparagraph (B) and each time the Attorney General and the Director materially change a directive under paragraph (1) issued to a covered electronic communication service provider that is not prohibited by subparagraph (B), the Attorney General and the Director shall provide the directive to the Foreign Intelligence Surveillance Court on or before the date that is 7 days after the date on which the Attorney General and the Director issue the directive, along with a description of the covered electronic communication service provider to whom the directive is issued and the

services at issue.

"(II) DUPLICATION NOT REQUIRED.—The Attorney General and the Director do not need to provide a directive or description to the Foreign Intelligence Surveillance Court under subclause (I) if a directive and description concerning the covered electronic communication service provider was previously provided to the Court and the directive or description has not materially changed.

"(ii) ADDITIONAL INFORMATION.—As soon as feasible and not later than the initiation of collection, the Attorney General and the Director shall, for each directive described in subparagraph (i), provide the Foreign Intelligence Surveillance Court a description of the type of equipment to be accessed, the nature of the access, and the form of assistance required pursuant to the directive.

"(iii) REVIEW.—

"(I) IN GENERAL.—The Foreign Intelligence Surveillance Act Court may review a directive received by the Court under clause (i) to determine whether the directive is consistent with subparagraph (B) and affirm, modify, or set aside the directive.

"(II) NOTICE OF INTENT TO REVIEW.—Not later than 10 days after the date on which the Court receives information under clause (ii) with respect to a directive, the Court shall provide notice to the Attorney General, the Director, and the covered electronic communication service provider, indicating whether the Court intends to undertake a review under subclause (I) of this clause.

"(III) COMPLETION OF REVIEWS.—In a case in which the Court provides notice under subclause (II) indicating that the Court intends to review a directive under subclause (I), the Court shall, not later than 30 days after the date on which the Court provides notice under subclause (II) with respect to the directive, complete the review.

"(E) CONGRESSIONAL OVERSIGHT.—

"(i) NOTIFICATION.—

"(I) IN GENERAL.—Subject to subclause (II), each time the Attorney General and the Director of National Intelligence issue a directive under paragraph (1) to a covered electronic communication service provider that is not prohibited by subparagraph (B) and each time the Attorney General and the Director materially change a directive under paragraph (1) issued to a covered electronic communication service provider that is not prohibited by subparagraph (B), the Attorney General and the Director shall submit to the appropriate committees of Congress the directive on or before the date that is 7 days after the date on which the Attorney General and the Director issue the directive, along with description of the covered electronic communication service provider to whom the directive is issued and the services at issue.

"(II) DUPLICATION NOT REQUIRED.—The Attorney General and the Director do not need to submit a directive or description to the appropriate committees of Congress under subclause (I) if a directive and description concerning the covered electronic communication service provider was previously submitted to the appropriate committees of Congress and the directive or description has not materially changed.

"(ii) ADDITIONAL INFORMATION.—As soon as feasible and not later than the initiation of collection, the Attorney General and the Director shall, for each directive described in subparagraph (i), provide the appropriate committees of Congress a description of the type of equipment to be accessed, the nature of the access, and the form of assistance required pursuant to the directive.

"(iii) REPORTING.—

"(I) QUARTERLY REPORTS.—Not later than 90 days after the date of the enactment of the Intelligence Authorization Act for Fiscal Year 2025 and not less frequently than once each quarter thereafter, the Attorney General and the Director shall submit to the appropriate committees of Congress a report on the number of directives issued, during the period covered by the report, under paragraph (1) to a covered electronic communication service provider and the number of directives provided during the same period to the Foreign Intelligence Surveillance Court under subparagraph (D)(i).

"(II) FORM OF REPORTS.—Each report submitted pursuant to subclause (I) shall be submitted in unclassified form, but may include a classified annex.

"(III) SUBMITTAL OF COURT OPINIONS.—Not later than 45 days after the date on which the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review issues an opinion relating to a directive issued to a covered electronic communication service provider under paragraph (1), the Attorney General shall submit to the appropriate committees of Congress a copy of the opinion.".

SEC. 1203. STRENGTHENING ELECTION CYBERSECURITY TO UPHOLD RESPECT FOR ELECTIONS THROUGH INDEPENDENT TESTING ACT OF 2024.

(a) Short Title.—This section may be cited as the "Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024" or the "SECURE IT Act of 2024".

(b) Requiring Penetration Testing as Part of the Testing and Certification of Voting Systems.—Section 231 of the Help America Vote Act of 2002 (52 U.S.C. 20971) is amended by adding at the end the following new subsection:

"(e) Required Penetration Testing.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Commission shall provide for the conduct of penetration testing as part of the testing, certification, decertification, and recertification of voting system hardware and software by the Commission based on accredited laboratories under this section.

"(2) ACCREDITATION.—The Commission shall develop a program for the acceptance of the results of penetration testing on election systems. The penetration testing required by this subsection shall be required for Commission certification. The Commission shall vote on the selection of any entity identified. The requirements for such selection shall be based on consideration of an entity's competence to conduct penetration testing under this subsection. The Commission may consult with the National Institute of Standards and Technology or any other appropriate Federal agency on lab selection criteria and other aspects of this program.".

(c) Independent Security Testing and Coordinated Cybersecurity Vulnerability Disclosure Program for Election Systems.—

(1) IN GENERAL.—Subtitle D of title II of the Help America Vote Act of 2002 (42 U.S.C. 15401 et seq.) is amended by adding at the end the following new part:

"PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS

"SEC. 297. INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS.

"(a) In General.—

"(1) ESTABLISHMENT.—The Commission, in consultation with the Secretary, shall establish an Independent Security Testing and Coordinated Vulnerability Disclosure Pilot Program for Election Systems (VDP–E) (in this section referred to as the 'program') to test for and disclose cybersecurity vulnerabilities in election systems.

"(2) DURATION.—The program shall be conducted for a period of 5 years.

"(3) REQUIREMENTS.—In carrying out the program, the Commission, in consultation with the Secretary, shall—

"(A) establish a mechanism by which an election systems vendor may make their election system (including voting machines and source code) available to cybersecurity researchers participating in the program;

"(B) provide for the vetting of cybersecurity researchers prior to their participation in the program, including the conduct of background checks;

"(C) establish terms of participation that—

"(i) describe the scope of testing permitted under the program;

"(ii) require researchers to—

"(I) notify the vendor, the Commission, and the Secretary of any cybersecurity vulnerability they identify with respect to an election system; and

"(II) otherwise keep such vulnerability confidential for 180 days after such notification;

"(iii) require the good faith participation of all participants in the program;

"(iv) require an election system vendor, within 180 days after validating notification of a critical or high vulnerability (as defined by the National Institute of Standards and Technology) in an election system of the vendor, to—

"(I) send a patch or propound some other fix or mitigation for such vulnerability to the appropriate State and local election officials, in consultation with the researcher who discovered it; and

"(II) notify the Commission and the Secretary that such patch has been sent to such officials;

"(D) in the case where a patch or fix to address a vulnerability disclosed under subparagraph (C)(ii)(I) is intended to be applied to a system certified by the Commission, provide—

"(i) for the expedited review of such patch or fix within 90 days after receipt by the Commission; and

"(ii) if such review is not completed by the last day of such 90-day period, that such patch or fix shall be deemed to be certified by the Commission, subject to any subsequent review of such determination by the Commission; and

"(E) 180 days after the disclosure of a vulnerability under subparagraph (C)(ii)(I), notify the Director of the Cybersecurity and Infrastructure Security Agency of the vulnerability for inclusion in the database of Common Vulnerabilities and Exposures.

"(4) VOLUNTARY PARTICIPATION; SAFE HARBOR.—

"(A) VOLUNTARY PARTICIPATION.—Participation in the program shall be voluntary for election systems vendors and researchers.

"(B) SAFE HARBOR.—When conducting research under this program, such research and subsequent publication shall be—

"(i) authorized in accordance with section 1030 of title 18, United States Code (commonly known as the 'Computer Fraud and Abuse Act'), (and similar State laws), and the election system vendor will not initiate or support legal action against the researcher for accidental, good faith violations of the program; and

"(ii) exempt from the anti-circumvention rule of section 1201 of title 17, United

States Code (commonly known as the 'Digital Millennium Copyright Act'), and the election system vendor will not bring a claim against a researcher for circumvention of technology controls.

"(C) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to limit or otherwise affect any exception to the general prohibition against the circumvention of technological measures under subparagraph (A) of section 1201(a)(1) of title 17, United States Code, including with respect to any use that is excepted from that general prohibition by the Librarian of Congress under subparagraphs (B) through (D) of such section 1201(a)(1).

"(5) DEFINITIONS.—In this subsection:

"(A) CYBERSECURITY VULNERABILITY.—The term 'cybersecurity vulnerability' means, with respect to an election system, any security vulnerability that affects the election system.

"(B) ELECTION INFRASTRUCTURE.—The term 'election infrastructure' means—

"(i) storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office; and

"(ii) related information and communications technology, including—

"(I) voter registration databases;

"(II) election management systems;

"(III) voting machines;

"(IV) electronic mail and other communications systems (including electronic mail and other systems of vendors who have entered into contracts with election agencies to support the administration of elections, manage the election process, and report and display election results); and

"(V) other systems used to manage the election process and to report and display election results on behalf of an election agency.

"(C) ELECTION SYSTEM.—The term 'election system' means any information system that is part of an election infrastructure, including any related information and communications technology described in subparagraph (B)(ii).

"(D) ELECTION SYSTEM VENDOR.—The term 'election system vendor' means any person providing, supporting, or maintaining an election system on behalf of a State or local election official.

"(E) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

"(F) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

"(G) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end of the items relating to subtitle D of title II the following:

"PART 7—Independent Security Testing and Coordinated Cybersecurity Vulnerability Disclosure Program for Election Systems

"Sec.297.Independent security testing and coordinated cybersecurity vulnerability disclosure program for election systems.".

SEC. 1204. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD QUALIFICATIONS.

Section 1061(h)(2) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(h)(2)) is amended by striking "and relevant experience" and inserting "or experience in positions requiring a security clearance, and relevant national security experience".

SEC. 1205. PARITY IN PAY FOR STAFF OF THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD AND THE INTELLIGENCE COMMUNITY.

Section 1061(j)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(j)(1)) is amended by striking "except that" and all that follows through the period at the end and inserting "except that no rate of pay fixed under this subsection may exceed the highest amount paid by any element of the intelligence community for a comparable position, based on salary information provided to the chairman of the Board by the Director of National Intelligence.".

SEC. 1206. MODIFICATION AND REPEAL OF REPORTING REQUIREMENTS.

(a) Briefing on Iranian Expenditures Supporting Foreign Military and Terrorist Activities.—Section 6705(a)(1) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412(a)(1)) is amended by striking ", and not less frequently than once each year thereafter provide a briefing to Congress,".

(b) Reports and Briefings on National Security Effects of Global Water Insecurity and Emerging Infectious Diseases and Pandemics.—Section 6722(b) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3024 note; division E of Public Law 116–92) is amended by—

(1) striking paragraph (2); and

(2) redesignating paragraphs (3) and (4) as paragraphs (2) and (3), respectively.

(c) Repeal of Report on Removal of Satellites and Related Items From the United States Munitions List.—Section 1261(e) of the National Defense Authorization Act for Fiscal Year 2013 (22 U.S.C. 2778 note; Public Law 112–239) is repealed.

(d) Briefing on Review of Intelligence Community Analytic Production.—Section 1019(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3364(c)) is amended by striking "December 1" and inserting "February 1".

(e) Repeal of Report on Oversight of Foreign Influence in Academia.—Section 5713 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3369b) is repealed.

(f) Repeal of Briefing on Iranian Expenditures Supporting Foreign Military and Terrorist Activities.—Section 6705 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (22 U.S.C. 9412) is amended—

(1) by striking subsection (b);

(2) by striking the enumerator and heading for subsection (a);

(3) by redesignating paragraphs (1) and (2) as subsections (a) and (b), respectively, and moving such subsections, as so redesignated, 2 ems to the left;

(4) in subsection (a), as so redesignated, by redesignating subparagraphs (A) and (B) as paragraphs (1) and (2), respectively, and moving such paragraphs, as so redesignated, 2 ems to the left; and

(5) in paragraph (1), as so redesignated, by redesignating clauses (i) through (v) as subparagraphs (A) through (E), respectively, and moving such subparagraphs, as so redesignated, 2 ems to the left.

(g) Repeal of Report on Foreign Investment Risks.—Section 6716 of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3370a) is repealed.

(h) Repeal of Report on Intelligence Community Loan Repayment Programs.—Section 6725(c) of the Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020 (50 U.S.C. 3334g(c)) is repealed.

(i) Repeal of Report on Data Collection on Attrition in Intelligence Community.—Section 306(c) of the Intelligence Authorization Act for Fiscal Year 2021 (50 U.S.C. 3334h(c)) is repealed.

SEC. 1207. TECHNICAL AMENDMENTS.

(a) Requirements Relating to Construction of Facilities to Be Used Primarily by Intelligence Community.—Section 602(a) of the Intelligence Authorization Act for Fiscal Year 1995 (50 U.S.C. 3304(a)) is amended—

(1) in paragraph (1), by striking "$6,000,000" and inserting "$9,000,000"; and

(2) in paragraph (2)—

(A) by striking "$2,000,000" each place it appears and inserting "$4,000,000"; and

(B) by striking "$6,000,000" and inserting "$9,000,000".

(b) Copyright Protection for Civilian Faculty of Certain Accredited Institutions.—Section 105 of title 17, United States Code, is amended to read as follows:

"105. Subject matter of copyright: United States Government works

"(a) In General.—Copyright protection under this title is not available for any work of the United States Government, but the United States Government is not precluded from receiving and holding copyrights transferred to it by assignment, bequest, or otherwise.

"(b) Copyright Protection of Certain Works.—Subject to subsection (c), the covered author of a covered work owns the copyright to that covered work.

"(c) Use by Federal Government.—

"(1) SECRETARY OF DEFENSE AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at a covered institution described in subparagraphs (A) through (K) of subsection (d)(2), the Secretary of Defense may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

"(2) SECRETARY OF HOMELAND SECURITY AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(L), the Secretary of Homeland Security may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

"(3) DIRECTOR OF NATIONAL INTELLIGENCE AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(M), the Director of National Intelligence may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

"(4) SECRETARY OF TRANSPORTATION AUTHORITY.—With respect to a covered author who produces a covered work in the course of employment at the covered institution described in subsection (d)(2)(N), the Secretary of Transportation may direct the covered author to provide the Federal Government with an irrevocable, royalty-free, worldwide, nonexclusive license to reproduce, distribute, perform, or display such covered work for purposes of the United States Government.

"(d) Definitions.—In this section:

"(1) COVERED AUTHOR.—The term 'covered author' means a civilian member of the faculty of a covered institution.

"(2) COVERED INSTITUTION.—The term 'covered institution' means the following:

"(A) National Defense University.

"(B) United States Military Academy.

"(C) Army War College.

"(D) United States Army Command and General Staff College.

"(E) United States Naval Academy.

"(F) Naval War College.

"(G) Naval Postgraduate School.

"(H) Marine Corps University.

"(I) United States Air Force Academy.

"(J) Air University.

"(K) Defense Language Institute.

"(L) United States Coast Guard Academy.

"(M) National Intelligence University.

"(N) United States Merchant Marine Academy.

"(3) COVERED WORK.—The term 'covered work' means a literary work produced by a covered author in the course of employment at a covered institution for publication by a scholarly press or journal.".