Calendar No. 412

118TH CONGRESS
2d Session

SENATE

REPORT
118–181

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2025

JUNE 12, 2024.—Ordered to be printed

Mr. WARNER, from the Select Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany S. 4443]

The Select Committee on Intelligence, having considered an original bill (S. 4443) to authorize appropriations for Fiscal Year 2025 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, the Central Intelligence Agency (CIA) Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

CLASSIFIED ANNEX TO THE COMMITTEE REPORT

Pursuant to Section 364 of the *Intelligence Authorization Act for Fiscal Year 2010* (Public Law 111–259), the Director of National Intelligence (DNI) publicly disclosed on March 12, 2024, that the request for the National Intelligence Program for Fiscal Year 2025 was $73.4 billion. Other than for limited unclassified appropriations, primarily the Intelligence Community Management Account, the classified nature of United States intelligence activities precludes any further disclosure, including by the Committee, of the details of its budgetary recommendations. Accordingly, the Committee has prepared a classified annex to this report that contains a classified Schedule of Authorizations. The classified Schedule of Authorizations is incorporated by reference in the *Intelligence Authorization Act for Fiscal Year 2025* and has the legal status of

public law. The classified annex is made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President. It is also available for review by any Member of the Senate subject to the provisions of Senate Resolution 400 of the 94th Congress (1976).

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the *Intelligence Authorization Act for Fiscal Year 2025* (the "Act") reported by the Committee.

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 specifies that the Act authorizes appropriations for intelligence and intelligence-related activities of the Intelligence Community (IC) for Fiscal Year 2025.

Section 102. Classified Schedule of Authorizations

Section 102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities for Fiscal Year 2025 are contained in the classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103. Intelligence Community Management Account

Section 103 authorizes appropriations for the Intelligence Community Management Account of the Office of the Director of National Intelligence (ODNI) for Fiscal Year 2025.

Section 104. Increase in employee compensation and benefits authorized by law

Section 104 provides that funds authorized to be appropriated by the 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 compensation or benefits authorized by law.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations for the CIA Retirement and Disability Fund for Fiscal Year 2025.

TITLE III—INTELLIGENCE COMMUNITY MATTERS

Section 301. Improvements relating to conflicts of interest in the Intelligence Innovation Board

Section 301 amends Section 7506 of the *Intelligence Authorization Act for Fiscal Year 2024,* which established the Intelligence Innovation Board, in order to improve the process for vetting potential conflicts of interest.

Section 302. National Threat Identification and Prioritization Assessment and National Counterintelligence Strategy

Section 302 amends Section 904 of the *Counterintelligence Enhancement Act of 2002* to update the process for submittal to Congress of the National Threat Identification and Prioritization Assessment and the National Counterintelligence Strategy.

Section 303. Open Source Intelligence Division of Office of Intelligence and Analysis personnel

Section 303 prohibits funds made available for Fiscal Year 2025 for the Office of Intelligence and Analysis of the Department of Homeland Security from being obligated or expended to increase the number of personnel assigned to the Open Source Intelligence Division who work exclusively or predominantly on domestic terrorism issues.

Section 304. Appointment of Director of the Office of Intelligence and Counterintelligence

Section 304 requires that the Director of the Office of Intelligence and Counterintelligence of the Department of Energy be appointed by the President, by and with the advice and consent of the Senate, for a six-year term.

Section 305. Improvements to advisory board of National Reconnaissance Office

Section 305 amends the composition of the Advisory Board of the National Reconnaissance Office (NRO) by permitting the Director of the NRO to independently appoint up to eight members to the Board. Section 305 also requires the Director to establish a charter for the Board and extends the Board until August 31, 2027.

Section 306. National Intelligence University acceptance of grants

Section 306 authorizes the National Intelligence University to accept qualifying research grants.

Section 307. Protection of Central Intelligence Agency facilities and assets from unmanned aircraft

Section 307 amends the *Central Intelligence Agency Act of 1949* to allow authorized CIA personnel to better detect and respond to threats posed to CIA facilities and assets by unmanned aircraft.

Section 308. Limitation on availability of funds for new controlled access programs

Section 308 prohibits funds made available for fiscal year 2025 for the National Intelligence Program from being obligated or expended for any controlled access program, until the head of the element of the IC responsible for the program submits the notification required by section 501A(b) of the *National Security Act of 1947.*

Section 309. Limitation on transfers from controlled access programs

Section 309 amends Section 501A(b) of the National Security Act of 1947 to prohibit the head of an element of the IC from transferring a capability from a controlled access program, until the head submits to the appropriate congressional committees and congres-

sional leadership notice of the intent of the head to make such transfer.

Section 310. Expenditure of funds for certain intelligence and counterintelligence activities of the Coast Guard

Section 310 authorizes the Commandant of the Coast Guard to use up to 1% of the amounts made available for the National Intelligence Program for each fiscal year for intelligence and counterintelligence activities of the Coast Guard relating to objects of a confidential, extraordinary, or emergency nature, which may be accounted for solely on the certification of the Commandant.

Section 311. Unauthorized access to intelligence community property

Section 311 establishes criminal penalties for unauthorized access to IC property.

Section 312. Strengthening of Office of Intelligence and Analysis

Section 312 amends Section 311 of Title 31 to establish within the Office of Terrorism and Financial Intelligence of the Department of Treasury, the Office of Economic Intelligence and Security, which replaces the Office of Intelligence and Analysis.

Section 313. Report on sensitive commercially available information

Section 313 requires each element of the IC to submit to the congressional intelligence committees an annual report on the access to, collection, processing, and use of sensitive commercially available information by such element. Section 313 further requires the DNI to make available to the public, once every 2 years, a report on the policies and procedures of the IC with respect to sensitive commercially available information.

Section 314. Policy on collection of United States location information

Section 314 requires the DNI, in coordination with the Attorney General, to issue a policy on the collection of United States location information by the IC.

Section 315. Display of flags, seals, and emblems other than the United States flag

Section 315 provides that any flag, seal, or emblem that is not the United States flag that is displayed at an official location of an element of the IC shall be smaller than the official United States flag and may not be displayed above the United States flag. Section 315 further provides that none of the funds made available by the *Intelligence Authorization Act 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 IC other than the United States flag or another authorized flag.

TITLE IV—COUNTERING FOREIGN THREATS

Subtitle A—People's Republic of China

Section 401. Strategy and outreach on risks posed by People's Republic of China smartport technology

Section 401 requires the Director of the National Counterintelligence and Security Center (NCSC) to engage with United States industry partners on the risks of smartport technology—including shipping and logistics infrastructure and software—of the People's Republic of China to United States supply chains and commercial activity.

Section 402. Assessment of current status of biotechnology of People's Republic of China

Section 402 requires the DNI, in consultation with the Director of the National Counterproliferation and Biosecurity Center (NCBC), to assess the current status of the biotechnology sector of the People's Republic of China. Within 30 days after the completion of the assessment, the DNI is required to submit a report on the findings to the congressional intelligence committees.

Section 403. Intelligence sharing with law enforcement agencies on synthetic opioid precursor chemicals originating in People's Republic of China

Section 403 requires the DNI, in consultation with the head of the Office of National Security Intelligence of the Drug Enforcement Administration and the Under Secretary of Homeland Security for Intelligence and Analysis, to 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. The DNI is further required to develop a mechanism for collaboration between the IC and other Federal Government agencies.

Section 404. Report on efforts of the People's Republic of China to evade United States transparency and national security regulations

Section 404 requires the DNI to submit to the congressional intelligence committees an unclassified report on the efforts of the People's Republic of China to evade specified national security restrictions and limitations.

Section 405. Plan for recruitment of Mandarin speakers

Section 405 requires the DNI to submit to the appropriate committees of Congress a comprehensive plan to prioritize the recruitment and training of individuals who speak Mandarin Chinese for each element of the IC.

Subtitle B—The Russian Federation

Section 411. Assessment of Russian Federation sponsorship of acts of international terrorism

Section 411 requires the DNI to conduct and submit to the appropriate congressional committees an assessment on the extent to

which the Russian Federation provides support for international acts of terrorism and cooperates with the antiterrorism efforts of the United States.

Section 412. Assessment of likely course of war in Ukraine

Section 412 requires the DNI, in collaboration with the Director of the Defense Intelligence Agency and the Director of the CIA, to submit to the congressional intelligence committees an assessment of the likely course of the war in Ukraine through December 31, 2025.

Subtitle C—International Terrorism

Section 421. Inclusion of Hamas, Hezbollah, Al-Qaeda, and ISIS officials and members among aliens engaged in terrorist activity

Section 421 amends Section 212 of the Immigration and Nationality Act to specify that any person who is a 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, is considered to be engaged in terrorist activities.

Section 422. Assessment and report on the threat of ISIS-Khorasan to the United States

Section 422 requires the Director of the National Counterterrorism Center to conduct an assessment of the threats to the United States and United States citizens posed by ISIS-Khorasan.

Section 423. Terrorist financing prevention

Section 423 requires the Secretary of the Treasury to submit to the President a report identifying any foreign financial institution or foreign digital asset transaction facilitator that has knowingly facilitated a significant financial transaction with a terrorist organization. Section 423 further requires the President to impose sanctions on such foreign financial institutions and foreign digital asset transaction facilitators.

Subtitle D—Other Foreign Threats

Section 431. Assessment of visa-free travel to and within Western Hemisphere by nationals of countries of concern

Section 431 requires the DNI to conduct and 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.

Section 432. Study on threat posed by foreign investment in United States agricultural land

Section 432 requires the DNI to conduct a study and provide a briefing to the appropriate committees of Congress on the threats posed to the United States by foreign investment in agricultural land in the United States.

Section 433. Assessment of threat posed by citizenship-by-investment programs

Section 433 requires the DNI and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury to complete an assessment on the threat posed to the United States by citizenship-by-investment programs. The DNI and the Assistant Secretary are further directed to submit a report to the appropriate congressional committees on the findings of the assessment and provide a briefing to such committees on the report.

Section 434. Mitigating the use of United States components and technology in hostile activities by foreign adversaries

Section 434 requires the DNI within 180 days of enactment to develop and commence implementation of a Supply Chain Risk Mitigation Strategy to mitigate or disrupt the acquisition and use of United States components in the conduct of activities harmful to national security. The DNI is further required to submit to Congress annually thereafter for three years a report on the status and effect of the strategy.

Section 435. Office of Intelligence and Counterintelligence review of visitors and assignees

Section 435 requires the Director of the Department of Energy's Office of Intelligence and Counterintelligence to establish procedures by which visitors and assignees are assessed for counterintelligence risks to research or activities undertaken at National Laboratories. It further requires the Director to advise a National Laboratory on visitors or assignees when the Director has reason to believe a visitor or assignee is a non-traditional collector, or when the Director has information indicating that the visitor or assignee constitutes a counterintelligence risk to a lab. Section 435 requires the Director to report quarterly to the appropriate congressional committees metrics regarding assignees and visitors admitted to the National Laboratories.

Section 436. Prohibition on National Laboratories admitting certain foreign nationals

Section 436 limits entry into Department of Energy National Laboratories by foreign nationals from China, Russia, Iran, North Korea, and Cuba, with an exception for legal permanent residents. Section 436 permits the Secretary of Energy, in consultation with the Director of the Office of Intelligence and Counterintelligence of the Department of Energy and certain senior counterintelligence officials at the Federal Bureau of Investigation (FBI), to waive the prohibition for nationals from these countries if the Secretary certifies that the benefits to the United States of access outweigh the national security and economic risks to the United States. Section 436 requires the Secretary to submit notifications to congressional committees of each waiver issued.

Section 437. Quarterly report on certain foreign nationals encountered at the United States border

Section 437 requires the Secretary of Homeland Security, in coordination with the DNI, to publish a quarterly report identifying the aggregate number of special interest aliens who have been en-

countered at or near the United States border and have been released, are under supervision, are being detained, or have been removed from the United States.

Section 438. Assessment of the lessons learned by the intelligence community with respect to the Israel-Hamas war

Section 438 requires the DNI to submit to the appropriate committees of Congress an assessment of the lessons learned from the Israel-Hamas war.

Section 439. Central Intelligence Agency intelligence assessment on Tren de Aragua

Section 439 requires the Director of the CIA to submit to the appropriate committees of Congress an assessment on the gang known as "Tren de Aragua."

Section 440. Assessment of Maduro regime's economic and security relationships with state sponsors of terrorism and foreign terrorist organizations

Section 440 requires the DNI to submit to the congressional intelligence committees an assessment of the economic and security relationships of the regime of Nicolás Maduro of Venezuela with specified state sponsors of terrorism and foreign terrorist organizations.

Section 441. Continued congressional oversight of Iranian expenditures supporting foreign military and terrorist activities

Section 441 requires the DNI to submit to the congressional intelligence committees a report describing the current occurrences, circumstances, and expenditures by Iran on military and terrorist activities outside the country.

TITLE V—EMERGING TECHNOLOGIES

Section 501. Strategy to counter foreign adversary efforts to utilize biotechnologies in ways that threaten United States national security

Section 501 requires the DNI, acting through NCBC, to develop and submit to the congressional intelligence committees a whole-of-government strategy to address concerns relating to biotechnologies.

Section 502. Improvements to the roles, missions, and objectives of the National Counterproliferation and Biosecurity Center

Section 502 expands NCBC's authorities, to include overseeing and coordinating the analysis of intelligence on biotechnologies.

Section 503. Enhancing capabilities to detect foreign adversary threats relating to biological data

Section 503 requires the DNI to take steps to standardize and enhance the capabilities of the IC to detect foreign adversary threats relating to biological data.

Section 504. National security procedures to address certain risks and threats relating to artificial intelligence

Section 504 requires the President to develop and implement procedures to facilitate information sharing on national security threats emanating from, or directed at, artificial intelligence systems.

Section 505. Establishment of Artificial Intelligence Security Center

Section 505 establishes an Artificial Intelligence Security Center within the National Security Agency, with functions that include making available a research test-bed to facilitate security research on artificial intelligence systems by private sector and academic researchers in a secure environment.

Section 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

Section 506 provides that it is the Sense of Congress that the IC should further explore the strategic use of private capital partnerships to secure enduring technological advantages for the IC and undertake regular consultation with Federal partners on best practices and lessons learned.

Section 507. Intelligence Community Technology Bridge Fund

Section 507 creates a fund to assist in transitioning IC products from the research and development phase to the contracting and production phase, with priority given to small business concerns and nontraditional defense contractors.

Section 508. Enhancement of authority for intelligence community public-private talent exchanges

Section 508 amends 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) to enhance the authority for exchanges between the private sector and the IC, with a focus on finance, acquisition, technology, innovation, and research.

Section 509. Enhancing intelligence community ability to acquire emerging technology that fulfills intelligence community needs

Section 509 enables the IC to use a streamlined acquisition process to acquire property, products, or services from companies that have completed an In-Q Tel work program in which the company furnished property, products, or services to address government technology needs or requirements.

Section 510. Management of artificial intelligence security risks

Section 510 requires the Director of the National Institute of Standards and Technology (NIST) to ensure that the National Vulnerability Database of the Institute incorporates artificial intelligence security vulnerabilities and addresses those vulnerabilities. It also directs NIST, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), to establish a database by which vendors can voluntarily disclose artificial intelligence secu-

rity and safety incidents. Finally, it directs the Director of CISA to ensure that the Common Vulnerabilities and Exposures Program encompasses artificial intelligence security vulnerabilities.

Section 511. Protection of technological measures designed to verify authenticity or provenance of machine-manipulated media

Section 511 prohibits the concealment, subversion, fraudulent distribution, and circumvention of technological measures designed to verify the authenticity, modifications, or conveyance of machine-manipulated media or characteristics of the provenance of such media. Section 511 also establishes civil penalties, enforceable by the Attorney General, for violations of the prohibitions.

Section 512. Sense of Congress on hostile foreign cyber actors

Section 512 provides that it is the sense of Congress that foreign ransomware organizations 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.

Section 513. Designation of state sponsors of ransomware and reporting requirements

Section 513 requires the Secretary of State, in consultation with the DNI, to annually designate as a state sponsor of ransomware any country the government of which the Secretary has determined provides support for ransomware demand schemes. Section 513 further requires the President to impose the sanctions and penalties imposed with respect to a state sponsor of terrorism on each country designated by the Secretary as a state sponsor of ransomware. Section 513 requires the Secretary of the Treasury to submit a report on 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. Section 513 also requires the Secretary of State to submit a report on the number and geographic locations of individuals, groups, and entities that identifies the country of origin of foreign-based ransomware attacks. Section 513 further requires the Comptroller General to issue a report on the authorities available to respond to foreign-based ransomware attacks.

Section 514. Deeming ransomware threats to critical infrastructure a national intelligence priority

Section 514 requires the DNI to deem ransomware threats to critical infrastructure a national intelligence priority component to the National Intelligence Priorities Framework. Section 514 further requires the DNI, in consultation with the Director of the FBI, to submit a report on the implications of the ransomware threat to United States national security.

TITLE VI—CLASSIFICATION REFORM

Section 601. Governance of classification and declassification system

Section 601 requires the President to designate an 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. Section 601 also requires the President to designate an official to establish policies and guidance relating to classification and declassification and controlled unclassified information and to oversee the implementation of such policies and guidance. Finally, Section 601 requires the President to establish an Executive Committee on Classification and Declassification Programs and Technology to provide direction, advice, and guidance to the Executive Agent.

Section 602. Classification and declassification of information

Section 602 authorizes the President to establish a system for the classification and declassification of information, subject to certain minimum requirements including the scope of information that may be classified, the duration of classification, and the processes for reviewing classified records and materials.

Section 603. Minimum standards for Executive agency insider threat programs

Section 603 requires each agency with access to classified information to establish an insider threat program that meets certain minimum standards, including establishing a capability to monitor user activity on all classified networks.

TITLE VII—SECURITY CLEARANCES AND INTELLIGENCE COMMUNITY WORKFORCE IMPROVEMENTS

Section 701. Security clearances held by certain former employees of intelligence community

Section 701 amends Section 803 of the National Security Act of 1947 to require the Security Executive Agent to 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 IC, but is no longer employed by the Federal Government, maintains a security clearance only in accordance with Executive Order 12968, or successor order. Section 701 also requires submission of the guidelines and instructions to Congress, as well as a report on former Presidential appointees who hold security clearances.

Section 702. Policy for authorizing intelligence community program of contractor-owned and contractor-operated sensitive compartmented information facilities

Section 702 requires the DNI to establish a standardized policy for the IC that authorizes a program of contractor-owned and contractor-operated sensitive compartmented information facilities as a service to the national security and intelligence enterprises.

Section 703. Enabling intelligence community integration

Section 703 authorizes the head of an element of the IC to provide goods or services to another element of the IC without reimbursement or transfer of funds for hoteling initiatives for IC employees and affiliates to enable those employees and affiliates to work from secure facilities maintained by other elements of the IC across a wide geographic area.

Section 704. Appointment of spouses of certain Federal employees

Section 704 amends Section 3330d of Title 5 to extend to spouses of an employee of the Department of State or an element of the IC the same options for federal employment as currently enjoyed by spouses of employees of the Department of Defense (DOD).

Section 705. Plan for staffing the intelligence collection positions of the Central Intelligence Agency

Section 705 requires the Director of the CIA to submit a plan for ensuring the Directorate of Operations has staffed every civilian full-time equivalent position authorized for that Directorate under the *Intelligence Authorization Act for Fiscal Year 2024*.

Section 706. Intelligence community workplace protections

Section 706 allows for IC incumbent personnel whose positions are converted involuntarily to the excepted service, or from one excepted service schedule to another, to retain their adverse action protections. Section 706 further requires congressional notification and explanation when heads of agencies terminate personnel in contravention of existing protections. Section 706 also prohibits the Director of the CIA from terminating an officer or employee except in accordance with guidelines and regulations submitted to the congressional intelligence committees, unless the Director determines that such compliance poses a threat to U.S. national security and provides an explanation for such determination to the committees.

Section 707. Sense of Congress on Government personnel support for foreign terrorist organizations

Section 707 establishes a 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, or continuous vetting of an individual for eligibility, certain enumerated actions shall be considered acts advocating an act of terrorism.

TITLE VIII—WHISTLEBLOWERS

Section 801. Improvements regarding urgent concerns submitted to Inspectors General of the intelligence community

Section 801 permits urgent concerns submitted by whistleblowers to the inspectors general of the IC to be provided directly to Congress rather than going through the heads of agencies when an inspector general determines that transmittal to the head of agency could compromise the anonymity of the employee or result in the complaint being transmitted to the subject of the complaint. Section 801 requires that submissions be made in writing and provides that the statutory review period for such submissions begins on the date the submitter confirms their written submission is complete,

while requiring the inspectors general to facilitate a writing of a submission or treat a written record of a verbal complaint as a submission. Finally, Section 801 clarifies that individuals formerly affiliated with an element of the IC may submit matters of urgent concern that arose during and related to the time of their prior employment with the element.

Section 802. Prohibition against disclosure of whistleblower identity as act of reprisal

Section 802 prohibits knowing or willful disclosures that reveal an IC employee's or IC contractor employee's identifying information without consent, so as to identify such employee or contractor employee as a whistleblower, except as necessary during the course of an investigation. Section 802 further establishes a private right of action for an IC whistleblower if such disclosure is taken as a reprisal against the whistleblower for bringing a complaint.

Section 803. Protection for individuals making authorized disclosures to Inspectors General of elements of the intelligence community

Section 803 clarifies that a disclosure of classified information to an Inspector General of an element of the IC that is made by a whistleblower who held a security clearance during the whistleblower's IC employment, but who, at the time of the disclosure, does not hold the appropriate clearance or authority to access such classified information, and that is otherwise made in accordance with such security standards and procedures, shall be treated as an authorized disclosure.

Section 804. Clarification of authority of certain Inspectors General to receive protected disclosures

Section 804 makes a technical correction to Section 1104 of the *National Security Act of 1947* to clarify that the inspectors general of defense intelligence elements are authorized recipients of whistleblower protected disclosures.

Section 805. Whistleblower protections relating to psychiatric testing or examination

Section 805 amends Section 1104 of the *National Security Act of 1947* to establish that a decision to order psychiatric testing or examination is a prohibited personnel practice when taken or threatened as a reprisal for a protected disclosure.

Section 806. Establishing process parity for adverse security clearance and access determinations

Section 806 requires an agency, in justifying an adverse security clearance or access determination against a whistleblower, to demonstrate by clear and convincing evidence that the agency would have made the same security clearance or access determination in the absence of the whistleblower's disclosure. Section 806 further establishes parity in the legal standards applied to IC whistleblower matters.

Section 807. Elimination of cap on compensatory damages for retaliatory revocation of security clearances and access determinations

Section 807 removes the cap on compensatory damages for an employee or former employee who was subjected to a reprisal with respect to the employee's or former employee's security clearance or access determination.

TITLE IX—ANOMALOUS HEALTH INCIDENTS

Section 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

Section 901 authorizes the Director of the CIA to pay or reimburse the costs relating to diagnosing or treating a qualifying injury that is not otherwise covered under existing law, under circumstances the Director determines to be extraordinary.

Section 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

Section 902 authorizes the Secretary of State or the head of any other Federal agency to pay or reimburse the costs relating to diagnosing or treating a qualifying injury that is not otherwise covered under existing law, under circumstances the Secretary (or relevant head of another Federal agency) determines to be extraordinary.

Section 903. Improved funding flexibility for payments made by Department of State for qualifying injuries to the brain

Section 903 improves funding flexibility for payments made by the Department of State for qualifying injuries to the brain.

TITLE X—UNIDENTIFIED ANOMALOUS PHENOMENA

Section 1001. Comptroller General of the United States review of All-domain Anomaly Resolution Office

Section 1001 requires the Comptroller General to conduct and submit a review of the All-Domain Anomaly Resolution Office regarding unidentified anomalous phenomena reporting and Federal agency coordination.

Section 1002. Sunset of requirements relating to audits of unidentified anomalous phenomena historical record report

Section 1002 terminates certain audit requirements of the unidentified anomalous phenomena historical record report.

Section 1003. Funding limitations relating to unidentified anomalous phenomena

Section 1003 maintains certain limitations on funding absent congressional oversight for Fiscal Year 2025.

TITLE XI—AIR AMERICA

Section 1101. Short title

Section 1101 provides that the title may be cited as the "Air America Act of 2024."

Section 1102. Findings

Section 1102 sets forth Congress's findings that Air America and its affiliated companies, in coordination with the CIA, supported the United States Government from 1950 to 1976, with service and sacrifice of its employees.

Section 1103. Definitions

Section 1103 sets forth the definitions of Air America affiliates, covered decedents, qualifying service, and other terminology.

Section 1104. Award authorized to eligible persons

Section 1104 authorizes the Director of the CIA to award payments to certain qualifying Air America employees and survivors, and sets forth eligibility requirements for award payments.

Section 1105. Funding limitation

Section 1105 sets a $60 million funding limitation, with the ability for the Director of the CIA to request additional funds to fulfill eligible award payments.

Section 1106. Time limitation

Section 1106 establishes a two-year time period within which claimants must file their award claims. The two-year period starts upon the date of Director of the CIA's application regulations, and upon receiving a claim, the Director has 90 days within which to make an eligibility determination.

Section 1107. Application procedures

Section 1107 requires the Director of the CIA to prescribe procedures for claimants to apply for award payments.

Section 1108. Rule of construction

Section 1108 clarifies that nothing in this subtitle shall entitle any person to Federal benefits under Title 5, chapters 81, 83, or 84.

Section 1109. Attorneys' and agents' fees

Section 1109 makes it unlawful for more than 25 percent of an award payment to be paid to, or received by, any agent or attorney for services rendered in connection with an award payment.

Section 1110. No judicial review

Section 1110 establishes that the Director of the CIA's determinations under this subtitle are not subject to judicial review.

Section 1111. Reports to Congress

Section 1111 requires the Director of the CIA to submit semiannual reports on the award payments made and denied (and, if a denial, the rationale therefor).

TITLE XII—OTHER MATTERS

Section 1201. Enhanced authorities for amicus curiae under the Foreign Intelligence Surveillance Act of 1978

Section 1201 enhances the authorities of court-appointed *amici* and establishes new requirements to appoint *amici* in a broader array of cases.

Section 1202. Limitation on directives under Foreign Intelligence Surveillance Act of 1978 relating to certain electronic communication service providers

Section 1202 provides that a directive may not be issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act to a covered electronic communication service provider, unless the covered provider is a provider of the type of service at issue in the opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review authorized for public release on August 23, 2023. Section 1202 also requires notification and reporting of information concerning such directives.

Section 1203. Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act of 2024

Section 1203 directs the Election Assistance Commission (EAC) to require that voting systems undergo penetration testing as part of the standard certification process for such systems. Section 1203 also directs the NIST to accredit entities that can perform such testing and directs the EAC to create a voluntary vulnerability disclosure program for election systems.

Section 1204. Privacy and Civil Liberties Oversight Board qualifications

Section 1204 amends the *Intelligence Reform and Terrorism Prevention Act of 2004* (42 U.S.C. § 2000ee(h)(2)) to ensure that experience in positions requiring a security clearance and relevant national security experience are among the qualifications that may be considered when appointing members of the Privacy and Civil Liberties Oversight Board. Section 1204 retains authority to consider expertise in civil liberties and privacy when appointing members to the Board.

Section 1205. Parity in pay for staff of the Privacy and Civil Liberties Oversight Board and the intelligence community

Section 1205 amends the *Intelligence Reform and Terrorism Prevention Act of 2004* (42 U.S.C. § 2000ee(j)(1)) to ensure that staff of the Privacy and Civil Liberties Oversight Board may be paid a rate of pay comparable to employees of the IC.

Section 1206. Modification and repeal of reporting requirements

Section 1206 modifies and repeals certain prior congressional intelligence committee reporting requirements that, for certain reasons, are no longer relevant or necessary to the congressional intelligence committees.

Section 1207. Technical amendments

Section 1207 makes certain technical amendments relating to IC facility construction and copyright permissions for works by the United States Government.

COMMITTEE COMMENTS AND DIRECTION

Intelligence, Surveillance, and Reconnaissance Oversight

The Committee is encouraged that DOD concurred with the recommendations outlined by the Government Accountability Office (GAO) in its October 2023 assessment of matters related to DOD's intelligence, surveillance, and reconnaissance (ISR) processing, exploiting, and disseminating (PED) capabilities (GAO–24–106088C), and is interested in the prompt implementation of these recommendations. The Committee notes that the ODNI did not respond to GAO's report, but recognizes the important coordination role that it should play in these matters. Consequently, the Committee directs the Office of the Secretary of Defense and ODNI to provide a briefing, 180 days after passage of the *Intelligence Authorization Act for Fiscal Year 2025*, to the congressional defense and intelligence committees, on the DOD implementation of recommendations made by the above-noted GAO report, and ODNI's support to these efforts. The briefing should include a discussion of the progress made by DOD, in coordination with ODNI, in implementing the recommendations in the GAO report, including any actions they have taken, challenges they face, and timelines for implementation. The briefing should also include a discussion of any proposals to the Congress that would streamline or otherwise improve efforts to address the recommendations.

Plan for Increased Security at United States Installations Used by Intelligence Community

At present, no unified plan across the IC exists for restricting access to transportation security companies accessing U.S. government facilities that house IC entities. While U.S. government installations generally have access requirements, including DOD, as described in 346(d) of the *National Defense Authorization Act for Fiscal Year 2017* (10 U.S.C. § 2661 note prec.), the IC has yet to clarify a congruent policy for all U.S. government installations that house IC components. The Committee remains concerned at potential counterintelligence gaps in access to U.S. installations that house IC entities and subsidiaries.

Therefore, the Committee directs that not later than 180 days after the date of the enactment of this Act, the DNI shall submit to the appropriate committees of Congress a plan to increase security at each installation under the control of the United States that is used by one or more elements of the IC, including by controlling access to such installations by any employee or contractor of a transportation company.

Establishing a National Intelligence Manager for Counternarcotics

In September 2023, the ODNI convened a 90-day Sprint Cell hosted by the National Counterterrorism Center (NCTC) to "identify opportunities to strengthen the IC integration of intelligence and support to policymakers and operators in disrupting the illicit

fentanyl supply chain." On April 2, 2024, the NCTC presented to Committee staff its report, which found that coordination between the IC and Federal Law Enforcement can be improved to enhance government-wide efforts to counter illicit fentanyl production and distribution. Therefore, the Committee directs the DNI to establish, within 90 days of enactment of this act, a National Intelligence Manager for Counternarcotics to focus exclusively on the counternarcotics mission.

China's attempts to exploit knowledge of proprietary U.S. tactics, techniques, and procedures

The Committee is concerned that our adversaries are targeting U.S. and allied servicemembers, and have successfully recruited former servicemembers, for employment in positions that allow adversaries to harvest knowledge and receive training on U.S., NATO, and allied military tactics, techniques and procedures (TTPs). These proprietary TTPs are a critical element of combat effectiveness that underpins our national security.

Therefore, to improve awareness of the threat and to develop mitigation strategies, the committee directs the DNI, working in coordination with the Under Secretary of Defense for Intelligence and Security, to undertake a review and report to the Committee, no later than 60 days after enactment, on (1) China's collection efforts and intended use of the information; (2) an assessment of the threat profile and related trends; and (3) recommended mitigating actions that can be taken across the targeted population including to protect U.S. servicemembers during and after their service, including veterans who operate commercial tactical training services. To contribute to public awareness, the report shall be unclassified to the maximum extent practicable, with a classified annex if needed.

Evolving Tactics of Transnational Criminal Organizations

Our national security is enhanced by continuing to strengthen border security in response to evolving threats. In recent years, transnational criminal organizations (TCOs), including those operating in Latin America and the border region, have leveraged technological developments and demonstrated an evolution in tactics in furtherance of narcotics trafficking and other activities that threaten national security. These have included the use of digital platforms, cryptocurrency and encrypted communication systems for a variety of activities, and testing the use of unmanned aerial vehicles to move drugs across the U.S. border and maritime transit routes.

Therefore, the Committee directs the DNI to brief the Committee, no later than 60 days after enactment, on (1) new tactics being utilized by TCOs, including leveraging digital technologies to include social media, cryptocurrency, and encrypted communications for recruitment and financial flows, and the use of unmanned underwater and aerial vehicles to facilitate surveillance and movement of materiel across maritime and land borders; (2) an assessment of the risk posed by these emergent capabilities; and (3) an assessment of resources necessary to support IC elements in addressing these developments.

Comptroller Review of Reporting and Response Procedures for Anomalous Health Incidents

The Committee is committed to ensuring continued investigation and research into anomalous health incidents (AHIs), and to the provision of appropriate medical care and compensation for individuals affected by such incidents. To achieve these aims, the U.S. government must have effective, standardized, and enforceable policies and procedures for reporting and responding to AHIs. However, the Committee is concerned that existing policies and procedures lack clarity and may be inconsistently applied across agencies and locations, potentially resulting in premature dismissals of AHIs without adequate diligence or process.

Therefore, the Committee directs the Comptroller General of the United States to conduct a review of the policies and procedures surrounding AHIs at U.S. government agencies, including but not limited to the IC, DOD, and Department of State. This review should evaluate:

1. The extent to which federal agencies have established and are following processes and procedures for consistent AHI reporting, evaluation, and response, consistent with section 6603 of the *National Defense Authorization Act for Fiscal Year 2022*.
2. The adequacy and consistency of agency and/or site-specific procedures and criteria at overseas and domestic locations for responding to, investigating, and evaluating the credibility of potential AHIs, including assessing disparities across agencies, location, and individual types (e.g. overseas vs. domestic, military vs. civilian employee, vs. contractor vs. dependent) and any mechanisms for appealing credibility determinations.
3. The extent to which each agency is collecting, storing, and sharing data regarding AHIs as outlined in current legislation, and the adequacy of the mechanisms to do so, including the government-wide database maintained by the NCSC.
4. How the data in the NCSC database are managed, shared across government, and used to support research, investigations, intelligence collection, and/or for other purposes.
5. Recommendations for improvements to existing policies, initiatives, and/or mechanisms to ensure efficient and consistent interagency coordination as it relates to the U.S. government's investigation of and response to AHIs.
6. Any other aspect relating to U.S. government's response to or treatment of AHIs that the Comptroller General deems appropriate.

The Committee further directs the Comptroller General to brief the Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence, Senate Armed Services Committee, House Armed Services Committee, Senate Foreign Relations Committee, and the House Foreign Relations Committee on preliminary observations not later than 90 days after the date of enactment of this Act, and to provide a final report at such time as is mutually agreed upon by the committees and the Comptroller General.

Annual Comptroller General Report on Cybersecurity and Surveillance Threats to Congress

Section 5710 of the *Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and*

2020 (P.L. 116–92), codified at 2 U.S.C. § 4111, requires the Comptroller General of the United States to submit to the congressional intelligence committees an annual report on cybersecurity and surveillance threats to Congress. For the next annual report conducted pursuant to this provision on cybersecurity and surveillance threats to the Senate, the Committee requests the Comptroller General to assess the following:

1. The extent to which the cryptography used in Senate collaboration platforms is consistent with leading cybersecurity practices, including those relating to end-to-end encryption.

2. Challenges that prevent offices or committees from implementing strong cryptography—such as end-to-end encryption—on Senate collaboration platforms.

3. Efforts taken by the Senate Sergeant at Arms (SAA) to safeguard the personal accounts, devices, and information of Senators, their staffs, and immediate families, and how those efforts compare to efforts taken by certain executive and judicial branch entities with statutory authority to safeguard the personal accounts, devices or information of employees.

4. The techniques, means, and methods used by the Senate SAA to detect surveillance against, hacks of, and the deployment of spyware by foreign governments, on mobile devices subject to Senate SAA cybersecurity safeguards, and how those techniques, means, and methods compare to those used by executive branch agencies to detect and protect against such cybersecurity and surveillance threats to mobile devices managed by those agencies.

As part of the report, the Comptroller General shall include any resulting recommendations to improve Senate policies and programs to meaningfully address related cybersecurity and surveillance threats and to protect Senate information.

In conducting the above assessments, the Committee suggests the Comptroller General consult with the Attorney General; the DNI, the Director of the Administrative Office of the United States Courts; the Director of the National Security Agency; the Secretaries of Defense, Homeland Security, and State; the Sergeant at Arms and Doorkeeper of the Senate and any other agencies the Comptroller General determines to have information necessary for conducting comprehensive assessments. The Committee expects these officials to fully cooperate with the Comptroller General and provide any information the Comptroller General determines is necessary to complete this work.

Intelligence Community Directive Oversight

Four years ago, ODNI updated the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (SCIFs) issued pursuant to Intelligence Community Directive 705. The Committee supports ODNI's efforts to ensure the Technical Specifications are regularly updated to account for changing and emerging technology. However, compliance with updated Technical Specifications also imposes costs on departments and agencies, as well as private industry, responsible for implementing the updated standards. These costs include those associated with displacing personnel and/or equipment from SCIF space in order to implement necessary physical upgrades.

Therefore, the Committee directs that not later than 180 days after the date of enactment of this Act, the DNI, in coordination with the Under Secretary for Defense for Intelligence and Security, submit to the congressional intelligence committees, the Committee on Armed Services of the Senate, and the Committee on Armed Services of the House of Representatives, a 5-year plan to communicate and implement the updated Technical Specifications. The briefing should include a threat background brief, and cost estimates for departments and agencies within the IC, and a plan to mitigate any loss of use of SCIF space resulting from renovations necessary to implement appropriate upgrades.

Committee Support for Ongoing Intelligence Community Collection, Analysis, and Research into Anomalous Health Incidents

As noted previously by the Committee's September 2022 organizational assessment of the National Counterintelligence and Security Center, the Committee is concerned about the emerging foreign intelligence threat landscape facing the IC. One of the key novel threats facing the IC workforce is AHIs. Many years after the first incidents were publicly reported, AHIs continue to be a vexing issue, as case definitions have proven elusive, and controversy has shrouded the results of analytical and research efforts to-date.

While most IC agencies assessed in March 2023 that AHIs reported by U.S. personnel to date were probably the result of factors that did not involve a foreign adversary—such as preexisting conditions, conventional illness, and environmental factors—the assessment acknowledged intelligence gaps and the existence of cases that could not be explained. The September 2022 IC Experts Panel also identified various research gaps and made a range of recommendations to help the U.S. government better understand, prevent, and manage AHIs, including calling for coordinated intelligence collection, data analysis, and research efforts across the U.S. government.

The Committee believes a whole-of-government approach is necessary to identify and mitigate novel personnel threats, including AHIs. To that end, the Committee, in the classified annex, directs the National Counterintelligence and Security Center to develop a strategy for next generation force protection; directs the CIA to redouble analytic efforts on emerging threats, including AHIs; and bolsters the budgets of several intelligence collection and research efforts focused on directed energy technology and next generation sensors.

The Committee also expresses support for ongoing Department of Defense initiatives related to AHIs, including establishing a registry of AHI reporters' medical data collected from the military health system and planning for acute stage, retrospective, and longitudinal studies of AHI reporters' medical conditions. The Committee directs IC agencies to provide robust support to these efforts as necessary and in accordance with the detailed direction in our classified annex.

COMMITTEE ACTION

On May 22, 2024, a quorum being present, the Committee met to consider the bill, classified annex, and amendments. The Committee took the following actions:

Votes on amendments to the committee bill and the classified annex

By unanimous consent, the Committee made the Chairman's and Vice Chairman's bill, together with the classified annex for Fiscal Year 2025, the base text for purposes of amendment.

By voice vote, the Committee adopted en bloc twenty-two amendments to the bill as follows: (1) an amendment by Chairman Warner, and cosponsored by Senators Collins and Cotton, to take actions against foreign ransomware actors and designate state sponsors of ransomware; (2) an amendment by Chairman Warner, and cosponsored by Senator Rounds, to prevent foreign terrorist financing regimes; (3) an amendment by Chairman Warner, and cosponsored by Vice Chairman Rubio, to make certain revisions to the Chairman's and Vice Chairman's bill regarding NCBC; (4) an amendment by Chairman Warner, and cosponsored by Vice Chairman Rubio, to make certain revisions to the Chairman's and Vice Chairman's bill regarding genomic data and biosurveillance capabilities; (5) an amendment by Chairman Warner, and cosponsored by Vice Chairman Rubio and Senator Casey, to strengthen the Office of Intelligence and Analysis; (6) an amendment by Vice Chairman Rubio to impose limitations on National Laboratories from admitting certain foreign nationals; (7) an amendment by Vice Chairman Rubio expressing the Sense of Congress on government personnel support for Foreign Terrorist Organizations; (8) an amendment by Vice Chairman Rubio to include Hamas, Hezbollah, Al-Qaeda, and ISIS officials and members among aliens engaged in terrorist activity; (9) an amendment by Vice Chairman Rubio to require a report on the threat of ISIS Khorasan to the United States; (10) an amendment by Vice Chairman Rubio limiting the display of flags, seals, and emblems other than the United States flag at IC facilities; (11) an amendment by Senator Wyden to require a report on sensitive commercially available information; (12) an amendment by Senator Wyden to require a policy on collection of United States location information; (13) an amendment by Senator Heinrich, and cosponsored by Senator Ossoff, regarding Foreign Intelligence Surveillance Act directives relating to certain electronic communication service providers; (14) an amendment by Senator Cotton to require continued oversight of Iranian expenditures supporting foreign military and terrorist activities; (15) an amendment by Senator Cotton to require a plan for staffing the CIA's intelligence collection positions; (16) an amendment by Senator Cornyn, and cosponsored by Chairman Warner and Senator Kelly, to make certain revisions to the Chairman's and Vice Chairman's bill regarding emerging technologies; (17) an amendment by Senator Moran regarding the Coast Guard's expenditure of funds for certain intelligence and counterintelligence activities; (18) an amendment by Senator Lankford to require reporting on certain foreign nationals encountered at the United States border; (19) an amendment by Senator Gillibrand to extend certain funding limitations relating to unidentified anomalous phenomena; (20) an amendment by Senator Ossoff, and cosponsored by Senators Wyden and Heinrich, to make certain technical revisions to the Chairman's and Vice Chairman's bill regarding Privacy and Civil Liberties Oversight Board members' qualifications; (21) an amendment by Senator Ossoff to make certain technical revisions to the Chairman's and Vice Chairman's bill regarding an assessment of the likely

course of war in Ukraine; and (22) an amendment by Senator Rounds, and cosponsored by Vice Chairman Rubio and Senators Risch, Moran, Cornyn, and Cotton, to prevent unauthorized access to IC property.

By unanimous consent, the Committee agreed to adopt a second-degree amendment by Senator Warner to his own amendment to protect technological measures designed to verify authenticity or provenance of machine-manipulated media. By voice vote, the Committee adopted Chairman Warner's amendment, as amended.

By unanimous consent, the Committee agreed to adopt a second-degree amendment by Senator Wyden to his own amendment providing certain protections, imposing reporting requirements on the IC regarding termination authorities, and prohibiting the Director of the CIA from terminating an officer or employee except in accordance with guidelines and regulations submitted to the congressional intelligence committees, unless the Director determines that such compliance poses a threat to U.S. national security and provides an explanation for such determination to the committees. By a vote of 10 ayes and 7 noes, the Committee adopted Senator Wyden's amendment, as amended. The votes in person or by proxy were as follows: Chairman Warner—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Bennet—aye; Senator Casey—aye; Senator Gillibrand—aye; Senator Ossoff—aye; Senator Kelly—aye; Vice Chairman Rubio—no; Senator Risch—no; Senator Collins—no; Senator Cotton—no; Senator Cornyn—no; Senator Moran—aye; Senator Lankford—no; Senator Rounds—no.

By voice vote, the Committee did not adopt an amendment by Senator Wyden to revise the definition of electronic communication service provider, as amended by the Reforming Intelligence and Securing America Act, with Senator Wyden recorded as an aye.

Senator Cornyn offered an amendment to strike the provision in the Chairman's and Vice Chairman's bill to revise the Foreign Intelligence Surveillance Act's *amicus curiae* authorities, and withdrew it pending future consideration.

By a vote of 9 ayes and 8 noes, the Committee adopted an amendment by Senator Ossoff to establish pay parity for Privacy and Civil Liberties Oversight Board staff with IC employees. The votes in person or by proxy were as follows: Chairman Warner—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Bennet—aye; Senator Casey—aye; Senator Gillibrand—aye; Senator Ossoff—aye; Senator Kelly—aye; Vice Chairman Rubio—no; Senator Risch—no; Senator Collins—no; Senator Cotton—no; Senator Cornyn—no; Senator Moran—no; Senator Lankford—no; Senator Rounds—no.

Votes to report the committee bill

On May 22, 2024, the Committee voted to report the bill, as amended, by a vote of 17 ayes and zero noes. The votes in person or by proxy were as follows: Chairman Warner—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Bennet—aye; Senator Casey—aye; Senator Gillibrand—aye; Senator Ossoff—aye; Senator Kelly—aye; Vice Chairman Rubio—aye; Senator Risch—aye; Senator Collins—aye; Senator Cotton—aye; Senator Cornyn—aye; Senator Moran—aye; Senator Lankford—aye; Senator Rounds—aye.

By unanimous consent, the Committee authorized the staff to make technical and conforming changes to the bill and classified annex.

COMPLIANCE WITH RULE XLIV

Rule XLIV of the Standing Rules of the Senate requires publication of a list of any "congressionally directed spending item, limited tax benefit, and limited tariff benefit" that is included in the bill or the committee report accompanying the bill. Consistent with the determination of the Committee not to create any congressionally directed spending items or earmarks, none have been included in the bill, the report to accompany it, or the classified schedule of authorizations. The bill, report, and classified schedule of authorizations also contain no limited tax benefits or limited tariff benefits.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to this legislation. On May 23, 2024, the Committee transmitted this bill to the Congressional Budget Office and requested an estimate of the costs incurred in carrying out the unclassified provisions.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee finds that no substantial regulatory impact will be incurred by implementing the provisions of this legislation.

CHANGES TO EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the Committee finds that it is necessary to dispense with the requirement of paragraph 12 to expedite the business of the Senate.

ADDITIONAL VIEWS OF VICE CHAIRMAN RUBIO, SENATOR RISCH, AND SENATOR ROUNDS

During the markup of the Fiscal Year 2025 Intelligence Authorization Act (IAA), the Committee adopted an amendment that purported to provide Intelligence Community (IC) employees with new employment protections, but in reality it will increase risks to America's national security and hinder the ability of Presidentially-appointed and Senate-confirmed IC officials to make personnel decisions to meet mission needs. We believe this provision—if enacted—will thwart the IC's effectiveness and upend decades of Congress's efforts to recognize the unique mission of the IC. Notably, the IC and Department of Defense (DOD) strongly oppose this amendment.

This amendment dictates to the heads of IC elements, specifically the Director of National Intelligence and the Director of the Central Intelligence Agency, as well as the Secretary of Defense, how to manage personnel decisions at their own agencies. The amendment restricts the ability of heads of IC elements from converting the employment status of their own personnel and mandates that IC employees in converted positions retain their competitive service rights under Title 5 even if the employee's position falls under the excepted service. The amendment further inhibits the Director of the Central Intelligence Agency from exercising termination authorities under Title 50 by imposing burdensome requirements to notify Congress about internal agency guidelines and regulations—which Congress intentionally declined to codify given the IC's unique national security mission and responsibilities.

Rather than protecting IC and certain DOD employees from adverse actions, the amendment micromanages the Senate-confirmed Directors' and Secretary's fundamental authorities and responsibilities to maintain their workforce in the interest of national security. The amendment requires congressional notifications upon conversion of competitive service positions to excepted service positions, or when the Director of the Central Intelligence Agency or the Secretary of Defense make certain termination decisions, which becomes a slippery slope toward unraveling the very specific and critical IC employment protections that Congress has legislated over the decades.

Congress recognized the Central Intelligence Agency's unique employment requirements by specifically exempting the Central Intelligence Agency from Title 5's requirements in 5 U.S.C. § 7511(b)(7). Congress further gave the Director of the Central Intelligence Agency full discretion to manage termination protocols, *see* 50 U.S.C. § 3036, and followed suit as to the Director of National Intelligence, *see* 50 U.S.C. § 3024. It was a long-debated, thoughtful process culminating in gradual codifications to ensure that America has the most efficient, effective, and capable men and

women protecting us from terrorism, counterintelligence threats, weapons of mass destruction, and many other national security perils that go unseen by the public.

The IC and DOD leadership, entrusted by the President of the United States and confirmed by the U.S. Senate, must be able to ensure the best and most capable personnel are in operational positions. They must be able to determine the right course of action when an employee's actions harm their employing agency, the workforce, or our national security. As to the DOD, the amendment would impose dual-track employment requirements, ultimately meaning that two respective employees serving in the same positions would be paid and treated differently.

Given all of the above, this amendment appears to be an attempt to impede future administrations' abilities to build a workforce that meets current critical national security challenges. There is no valid problem that this amendment is attempting to solve.

MARCO RUBIO.
JAMES E. RISCH.
M. MICHAEL ROUNDS.

ADDITIONAL VIEWS OF SENATOR WYDEN

The Intelligence Authorization Act for Fiscal Year 2025 includes critical protections for Intelligence Community personnel against political firings and whistleblower reprisals.

My amendment to the bill ensures that personnel who are involuntarily moved from one employment status to another can retain their protections from firing. The amendment also ensures that if an Intelligence Community employee is fired without any due process, as is currently authorized, the agency must explain its reasons to Congress. This oversight is critical to protecting against politically motivated firings and preserving the independence and professionalism of the Intelligence Community.

The bill includes a number of provisions I submitted protecting Intelligence Community whistleblowers. One provision allows classified whistleblower complaints to be provided directly to Congress if the Inspector General determines that sending the complaint to the whistleblower's agency, as the statute currently requires, could compromise the anonymity of the whistleblower or result in the complaint being delivered to the subject of that complaint. Other provisions ensure that whistleblowers can't have their security clearances revoked on a pretext; allow for former Intelligence Community employees to submit whistleblower complaints; remove the cap on damages for retaliatory revocation of whistleblowers' clearances; and prohibit, as acts of reprisal, public disclosures of whistleblowers' identities as well as orders to undertake psychological examinations.

The bill includes two of my amendments that increase oversight of and public reporting on the Intelligence Community's collection of Americans' private data. Since the beginning of this administration, I have pressed the Intelligence Community to be transparent about its purchases of sensitive data on Americans. On May 8, 2024, the Office of the Director of National Intelligence released the Intelligence Community Policy Framework for Commercially Available Information. While I was disappointed that the Framework did not prohibit the Intelligence Community from purchasing any particular type of information, it did require IC elements to report to the ODNI on its purchases of sensitive information on Americans, while directing IC elements to employ privacy-protecting safeguards. My amendment requires an annual report to Congress on the Intelligence Community's access to and collection, purchase and use of commercial datasets that contain sensitive data on Americans, as well as its implementation of the safeguards. The amendment also codifies the Framework's requirement of a public report every two years.

In the years since the 2018 U.S. Supreme Court case of *Carpenter v. United States*, the Intelligence Community's policies with regard to the warrantless collection of U.S. location data have been

both inconsistent and opaque. My amendment to the bill brings clarity to this long-standing problem by requiring the Intelligence Community to issue a public policy on its collection of U.S. location information.

For years, I have worked to reform the country's broken classification and declassification system. In particular, I have joined with Senator Jerry Moran to ensure that there be an Executive Agent for Classification and Declassification to lead a fully integrated, U.S. government-wide reform effort. My provision directs the President to designate an Executive Agent and provide a clear funding plan for governing the reform process, including money for the perpetually under-resourced Public Interest Declassification Board.

The bill modifies the Foreign Intelligence Surveillance Act (FISA) in several ways. In April 2024, as the Senate considered the Reforming Intelligence and Securing America Act (RISAA), I sought to strike from the bill a sweeping new definition of electronic communications service provider that would authorize the government to force almost any American with access to a server, a wire, a cable box or wifi to participate in warrantless surveillance under Section 702 of FISA. At the time, the Department of Justice stated that it would only apply the new authorities to the type of service provider at issue in a 2023 FISA Court case. However, no such limitation was in the statute.

The Intelligence Authorization Act represents a significant improvement, codifying that limitation and adding provisions allowing for FISA Court review and congressional oversight of the new authorities. However, the actual boundaries of what is legal under the new authorities remain hidden from the public. It is a fundamental democratic principle that an American citizen should be able to read the law and have some inkling about what the government is and is not permitted to do, particularly when it comes to warrantless surveillance.

For this reason, I offered an amendment to replace the new authorities with a clear articulation of which providers are now subject to Section 702. This amendment would have allowed the public to understand the intent and effect of the new surveillance authorities, while permitting an informed, open debate in Congress when these authorities sunset in 2026. The defeat of my amendment unfortunately perpetuates secret law, a problem that undermines trust in government and the Congress. Voters have a need and a right to understand the limits of what is and is not permitted under the law, so that they can ratify or reject decisions that elected officials make on their behalf.

The bill includes a provision strengthening the role of the amicus curiae in the FISA Court. Many of these reforms originated in the USA RIGHTS Act, which I introduced in 2017 with a bipartisan, bicameral coalition. In 2020, they passed the Senate by a 77–19 vote thanks to the leadership of Senators Lee and Leahy, although they were not passed into law at that time. I commend Chairman Warner and Vice Chairman Rubio for continuing to push for these important reforms and for including them in this bill.

Finally, the bill includes a provision granting the Attorney General new powers to police the labeling of AI-generated media. This

provision is modeled on the Digital Millennium Copyright Act's anti-circumvention provisions, which are extremely controversial and have chilled legitimate cybersecurity research. The use of this problematic legislative framework to address the cutting-edge issue of AI-generated media raises numerous First Amendment and other questions that need to be considered and debated in public. I am also concerned about a blanket exemption for intelligence agencies as well as law enforcement, state actors and contractors at all levels to use unlabeled deepfake material.

RON WYDEN.

ADDITIONAL VIEWS OF SENATOR HEINRICH

The Intelligence Authorization Act for Fiscal Year 2025 that the Senate Intelligence Committee reported out on May 22, 2024, includes a provision I drafted that would limit the new definition of Electronic Communication Service Provider (ECSP) in the Reforming Intelligence and Securing America Act (RISAA) to providers of the type of service at issue in the 2023 FISA Court and FISA Court of Review opinions. The language was part of a managers' amendment that was accepted with bipartisan support.

My provision is intended to be consistent with the statement in the Assistant Attorney General letter of April 17, 2024, that: "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 [Foreign Intelligence Surveillance Court]." The letter went further to explain that "[t]he number of technology companies providing this service is extremely small."

My provision is also intended to be consistent with the clarification in the Explanatory Statement to accompany RISAA that "Congress intends that the amended ECSP definition will be used exclusively to cover the type of service provider at issue in the litigation before the FISC."

I also supported an amendment to the Intelligence Authorization Act that would prohibit the intentional, deceptive removal of content provenance information, such as a watermark, label, or metadata attached to an image that demonstrates where it came from. As the quality and availability of AI-powered digital content generation tools increases, content provenance information will be an increasingly important basis of trust in the online information ecosystem.

The amendment takes an enforcement approach based on civil actions against end users that deceptively remove content provenance information (or providers of software that help enable this removal). In order to truly address the problem of online disinformation at scale, however, I believe the bulk of the responsibility lies with online content distributors and social media platforms to ensure that content provenance information is available and transmitted faithfully, rather than with end users.

MARTIN HEINRICH.

○