AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 420

119TH CONGRESS
2d Session

SENATE

REPORT
119–133

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2027

AUGUST 5, 2026.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 4615]

The Select Committee on Intelligence, having considered an original bill (S. 4615) to authorize appropriations for Fiscal Year 2027 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account (ICMA), 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 April 21, 2026, that the request for the National Intelligence Program (NIP) for Fiscal Year 2027 was $81.9 billion. Other than for limited unclassified appropriations, 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 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 2027* and has the legal status of public law. The classified annex is made available to the Commit-

tees 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), as amended, and the Rules of Procedure for the Committee.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the *Intelligence Authorization Act for Fiscal Year 2027* (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 2027.

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 2027 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 ICMA of the Office of the Director of National Intelligence (ODNI) for Fiscal Year 2027.

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 2027.

TITLE III—MATTERS RELATING TO THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 301. Appointment of Deputy Director of National Intelligence and Assistant Directors of National Intelligence

Section 301 redesignates the Principal Deputy Director of National Intelligence as the Deputy Director of National Intelligence, and the current Deputy Directors of National Intelligence as Assistant Directors of National Intelligence.

Section 302. Repeal of National Intelligence Management Council

Section 302 amends the *National Security Act of 1947* to repeal the statute codifying establishment of the National Intelligence Management Council.

Section 303. Repeal of various positions, units, centers, councils, and offices

Section 303 amends the *National Security Act of 1947* to repeal the office of IC Chief Data Officer, the Intelligence Community Innovation Unit, the Framework for Cross-Disciplinary Education and Training, the Foreign Languages Program, and the Joint Intelligence Community Council.

Section 304. Transfer of National Intelligence University

Section 304 transfers the statutory functions of the National Intelligence University (NIU) to the National Defense University (NDU).

Section 305. Limitation on domestic activities at the National Counterterrorism Center

Section 305 amends the *National Security Act of 1947* to permit the National Counterterrorism Center (NCTC) to receive and retain intelligence pertaining to domestic terrorism to enable NCTC to collect, retain, and disseminate intelligence pertaining only to international terrorism.

Section 306. Timely provision of security direction to intelligence community whistleblowers

Section 306 requires the relevant Inspectors General to provide security guidance to whistleblowers within seven calendar days of notification that the whistleblower intends to contact the intelligence committees.

Section 307. Notification of certain declassifications

Section 307 amends the *National Security Act of 1947* to mandate that the DNI notify the congressional intelligence committees and the Archivist if the DNI exercises her authority under section 3.1(c) of Executive Order 13526 to declassify or downgrade properly classified information. Section 307 also requires each IC element to notify the congressional intelligence committees and the Archivist if the element exercises the authority under section 3.1(d) of Executive Order 13526 to declassify information where the need to protect such information is outweighed by the public interest in disclosure.

Section 308. No Police, Subpoena, or Law Enforcement Powers or Internal Security Functions for Director of National Intelligence

Section 308 establishes that the DNI has no police, subpoena, or law enforcement powers or internal security functions.

TITLE IV—MATTERS RELATING TO THE CENTRAL INTELLIGENCE AGENCY

Section 401. Extension of Central Intelligence Agency authority regarding unmanned aircraft systems

Section 401 extends the CIA's authority to allow authorized CIA personnel to better detect and respond to threats posed to CIA facilities and assets by unmanned aircraft, to align with other Federal agencies' similar authorities.

Section 402. Higher Education Act of 1965 special rule

Section 402 makes a technical correction to the *Higher Education Act of 1965*, as amended by Section 7316 of the *Intelligence Authorization Act for Fiscal Year 2024*, with respect to officers or employees of elements of the IC.

Section 403. Modification relating to security personnel at certain installations

Section 403 amends the *Central Intelligence Agency Act of 1949* to authorize the CIA to exercise law enforcement jurisdiction over certain National Reconnaissance Office (NRO) facilities.

TITLE V—MATTERS RELATING TO OTHER ELEMENTS OF THE INTELLIGENCE COMMUNITY

Section 501. Authority of National Security Agency to correlate, evaluate, and disseminate certain intelligence

Section 501 permits the Director of the National Security Agency (NSA) to correlate, evaluate, and disseminate intelligence related to national security.

Section 502. Prohibition on availability of funds for relocation of Office of Intelligence and Analysis to certain facilities

Section 502 prohibits NIP funds from being used to move or relocate the Department of Homeland Security's Office of Intelligence and Analysis (DHS I&A) to any facility other than a facility owned by DHS.

Section 503. Funds for foreign intelligence activities conducted with and by the National Reconnaissance Office

Section 503 permits the NRO to use appropriated funds for intelligence and communications purposes to pay for the arrangements with foreign countries for intelligence activities conducted by the NRO. Section 503 further permits the NRO to use funds other than appropriated funds for such arrangements in certain limited circumstances.

Section 504. Modification of annual report on Federal Bureau of Investigation case data

Section 504 clarifies a Federal Bureau of Investigation (FBI) reporting requirement regarding terrorist organizations.

Section 505. Establishment of Office of Counterintelligence

Section 505 establishes an Office of Counterintelligence within the Department of Treasury's Office of Intelligence and Analysis.

Section 506. Modification of responsibilities of Office of Intelligence and Analysis

Section 506 amends the *Homeland Security Act of 2002* to require that the activities of the DHS I&A have a foreign intelligence or counterintelligence nexus, prohibits collection of intelligence or information on U.S. persons, and changes the scope of I&A's responsibilities from terrorism to foreign threats to the homeland.

Section 507. Role of National Security Agency in collection and analysis of signals intelligence

Section 507 establishes that the Director of the NSA will provide direction for and coordination of signals intelligence activities across the IC, and will coordinate with other departments, agencies, and elements of the United States Government authorized to undertake signals intelligence activities to ensure effective use of resources and risk assessment for such activities.

TITLE VI—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 601. Amendments to presidential appointments for intelligence community positions

Section 601 amends the requirements for Presidential appointments and Senate confirmation of certain IC positions.

Section 602. Procedures regarding dissemination of nonpublicly available information concerning United States persons

Section 602 codifies IC Policy Guidance 107.1, which requires each IC element to develop procedures for responding to unmasking requests.

Section 603. Analytic standards for all-source intelligence products

Section 603 codifies IC Directive 203, which establishes analytic tradecraft requirements for all-source intelligence products.

Section 604. Limitation on use of Intelligence Community Management Account funds for certain entities

Section 604 prohibits ICMA funds from being used to support analytic collaboration efforts by non-profit entities that receive funds from foreign governments (with the exception of the Five Eyes), or by certain research or advocacy organizations that receive funds from foreign adversaries.

Section 605. Ben Sasse Intelligence Community Technology Fellowship Program

Section 605 creates a fellowship named after Senator Ben Sasse for IC employees to gain experience at technology companies and bring that experience back to their home agencies.

Section 606. Intelligence Community Counterintelligence Office at the Department of Commerce

Section 606 directs the establishment of the Intelligence Community Counterintelligence Office within the Department of Commerce.

Section 607. Countering hostile foreign cyber actors as a national intelligence priority

Section 607 requires the DNI and the Director of the FBI to prepare a report on hostile foreign cyber actors, including foreign scam centers.

Section 608. Notification of criminal referrals regarding current or former intelligence community employees

Section 608 requires the General Counsel of an element of the IC to notify the congressional intelligence committees if that element makes a criminal referral of a current or former IC employee to the Department of Justice.

Section 609. Modification of definitions in National Security Act of 1947 and scope of intelligence sharing responsibilities of Director of National Intelligence

Section 609 amends the *National Security Act of 1947* to limit the definition of "intelligence" to foreign intelligence and counterintelligence. Section 609 also limits the definition of "national intelligence" and "intelligence related to national security" to intelligence involving foreign threats to the United States. Section 609 further amends the *National Security Act of 1947* to clarify that the DNI can share intelligence with other Federal agencies.

Section 610. Prohibition on intelligence community use of adversary unmanned ground vehicles

Section 610 prohibits the IC from procuring or operating autonomous ground vehicles from the People's Republic of China (PRC or China), the Russian Federation (Russia), the Islamic Republic of Iran (Iran), or the Democratic People's Republic of Korea (DRPK), with limited exemptions.

Section 611. China-Taiwan Strategic Warning Task Force

Section 611 requires the DNI and Undersecretary of Defense for Intelligence and Security to establish a task force to coordinate efforts to provide indications and warning of any military aggression by the PRC against Taiwan.

Section 612. Limitations relating to Chinese products and services

Section 612 amends Section 6604 of the *Intelligence Authorization Act for Fisal Year 2026* to expand the scope of covered applications that are required to be removed from national security systems to include any product or service from any entity of the PRC that is included on the Entity List maintained by the Bureau of Industry and Security of the Department of Commerce, the Non-SDN Chinese Military-Industrial Complex Companies List, or the list of Chinese military companies required under Section 1260H of the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*. Section 612 further amends Section 414 of the *Intelligence Authorization Act for Fiscal Year 2022* to prohibit all IC elements from procuring certain information or communication technology products manufactured in China, Hong Kong, or Macau, or a product or service provided by an entity that is fully or partially owned or controlled by, or otherwise connected to, the government of China, without first completing a security assessment.

Section 613. Limitation on intelligence community support for offensive cyber operations conducted by nongovernmental entities

Section 613 prohibits the IC from providing intelligence or support for offensive cyber operations by nongovernmental entities not operating under IC or presidential authorities.

Section 614. Biological intelligence activities of the intelligence community

Section 614 requires the DNI, in coordination with the Secretary of Defense, to determine which elements of the IC would benefit by receiving anonymized biological data and intelligence regarding foreign biological threats and to disseminate such data and intelligence to those agencies. Section 614 further requires the DNI, in coordination with the Secretary of Defense, to ensure standards regarding anonymized biological data and information collection are consistent with other Federal agencies and to facilitate access to relevant IC databases.

Section 615. Prohibition on participation in prediction markets

Section 615 prohibits IC employees, contractors, and former employees and contractors who hold a security clearance from participating in prediction markets relating to any nonpublic information to which they had access by virtue of their employment and clearance status. Section 615 further provides that such prohibition extends two years after the individual leaves their employment or contract with the IC.

Section 616. Repeal of certain report and briefing requirements

Section 616 repeals unnecessary, outdated, or duplicative reporting and briefing requirements.

Section 617. Intelligence community personnel travel, allowances, and related expenses regulations

Section 617 directs the Director of the CIA to review its travel regulations and report to the congressional intelligence committees with recommended changes. Section 617 further instructs the DNI to biennially review travel procedures and submit reports to the congressional intelligence committees with recommendations for changes necessary to carry out intelligence functions.

Section 618. Prohibition on sending and receiving objects using entities owned or controlled by persons or governments of certain countries

Section 618 instructs the DNI to develop a list of products and technologies that affect American national security and prohibits the IC from sending or receiving these items using shipping companies that are controlled or owned by persons or government entities domiciled in the PRC, Russia, Iran, or the DPRK.

Section 619. Enhancing intelligence cooperation in the Indo-Pacific region

Section 619 directs the DNI, in coordination with Five Eyes nations, to improve intelligence cooperation with regional partners and allies.

Section 620. Intelligence activities related to Ukraine

Section 620 directs the DNI, in coordination with the heads of the IC elements, to ensure intelligence support to Ukraine through the duration of the conflict with Russia and to notify the congressional intelligence committees if the DNI decides to materially reduce intelligence support. Section 620 provides that, if Russia and Ukraine agree to end the conflict, the DNI must adjust intelligence sharing to support implementation of that agreement and to maintain and build Ukrainian defense capability. Section 620 further requires reporting on the resolution and Ukraine's status. Section 620 also directs the DNI to provide Ukraine and members of the North Atlantic Treaty Organization (NATO) early warning of potential Russian aggression against Ukraine.

Section 621. Requirements relating to intelligence sharing with countries of significant concern to the United States

Section 621 directs the DNI to notify the congressional intelligence committees if intelligence support is restricted or materially downgraded regarding Israel, Ukraine, Taiwan, or other countries designated by the President.

Section 622. United States-Israel intelligence sharing enhancement

Section 622 directs the President to expand and enhance intelligence sharing with Israel, limits reductions in intelligence sharing, and requires notice to the congressional intelligence committees of any material changes to intelligence sharing. Section 622 further directs the President to expand intelligence sharing with Abraham Accord countries. Finally, Section 622 requires the President to submit a report to the congressional intelligence committees annually for five years describing these intelligence sharing relationships.

TITLE VII—ARTIFICIAL INTELLIGENCE MATTERS RELATED TO THE INTELLIGENCE COMMUNITY

Section 701. Artificial intelligence exploitation guard and intelligence sharing

Section 701 establishes a three-year pilot program run by the NSA's Artificial Intelligence Security Center (AISC) to facilitate sharing intelligence and threat information with frontier artificial intelligence (AI) developers.

Section 702. Director of National Intelligence review of intelligence community use of artificial intelligence to support targeting

Section 702 directs the DNI to conduct a review and submit a report to the congressional intelligence committees identifying and describing the IC's use of AI tools in the lethal targeting cycle and to issue policies to mitigate identified risks.

Section 703. Improvements for artificial intelligence policies, standards, and guidance for intelligence community

Section 703 directs the Chief Artificial Intelligence Officer of the IC to review the IC's policies for labeling intelligence information generated or modified by AI and the adequacy of access-management systems for information used by agentic AI systems. Section

703 further directs the DNI to issue policy guidance on the use of agentic AI systems.

Section 704. Additional functions and requirements of Artificial Intelligence Security Center

Section 704 directs the AISC to make available a research testbed to private sector and academic researchers to engage in AI security research, including pre-deployment testing of AI models.

Section 705. Reports on novel uses of artificial intelligence technology

Section 705 requires the DNI to submit recurring reports to the congressional intelligence committees detailing any novel use of AI technology in advance of that technology's deployment within the IC.

Section 706. Clear labeling of artificial intelligence outputs for targeting workflows

Section 706 requires the DNI to establish a policy that requires labeling of outputs from AI systems that are used to develop or inform lethal targeting.

Section 707. Research on use of artificial intelligence relating to inadvertent escalation

Section 707 requires Intelligence Advanced Research Projects Activity (IARPA) to research the specific ways in which the IC's use of AI could contribute to inadvertent escalation and report the findings to the congressional intelligence committees.

Section 708. Research on interaction of adversarial artificial intelligence systems with intelligence community systems

Section 708 requires IARPA to research novel dynamics and vulnerabilities that may arise from the interaction of adversarial AI systems with the IC's AI systems and report the findings to the congressional intelligence committees.

Section 709. Proliferation assessments regarding the export of artificial intelligence-related technologies

Section 709 requires the DNI to provide to the President and the congressional intelligence committees an analysis of the risks associated with granting a license for the export of AI technology at least 90 days before the Secretary of Commerce grants such a license.

Section 710. Review of artificial intelligence security vulnerabilities under Vulnerabilities Equities Process

Section 710 directs the Director of the NSA to evaluate the sufficiency of the Vulnerabilities Equities Process (VEP) in identifying AI vulnerabilities. Section 710 further directs the Director to provide reports and a briefing to Congress regarding its evaluation of the VEP as it relates to AI.

Section 711. Prohibition on certain artificial intelligence models on intelligence community systems

Section 711 prohibits the IC from using AI systems that have been found to have generated child sexual abuse material or nonconsensual intimate images of adults. Section 711 further requires such models to be removed from IC networks unless the IC can implement safeguards or the model's provider cures its defects.

TITLE VIII—OTHER MATTERS

Section 801. Modification to notification requirements for authorized and ordered departures

Section 801 requires the Department of State to inform the congressional intelligence and national security committees if an American embassy is subject to an authorized or ordered departure.

Section 802. Identification of reallocable frequencies

Section 802 amends the authorization of the Spectrum Relocation Fund to clarify eligibility for Title 50 agencies that utilize spectrum and whose usage could be impacted by future reallocation decisions.

Section 803. Protection of classified information relating to budget functions

Section 803 requires the Executive Branch to use secure systems for NIP budget functions, including obligating and expending funds, performing financial management services, and developing and submitting budget materials to Congress.

Section 804. Review by Committee on Foreign Investment in the United States of transactions in real estate near intelligence community facilities

Section 804 directs the Committee on Foreign Investment in the United States to review real estate transactions involving a foreign person or entity near IC facilities.

Section 805. Intelligence support to the U.S. International Development Finance Corporation

Section 805 requires the DNI to provide intelligence support to the U.S. International Development Finance Corporation.

Section 806. Establishing processes and procedures for protecting Federal Reserve information

Section 806 requires the DNI, in coordination with the Director of the FBI, to work with the Chair of the Board of Governors of the Federal Reserve System to implement security measures for protecting information collected or generated by the Federal Reserve.

Section 807. Amendments to prohibit payments to obtain national security information or approvals

Section 807 amends the *Export Control Reform Act of 2018*, the *Protecting Americans from Foreign Adversary Controlled Applications Act,* and the *National Security Act of 1947* to prohibit pay-

ments to obtain national security licenses, authorizations, or access to classified information.

Section 808. Offenses involving espionage

Section 808 removes the statute of limitations for certain espionage offenses.

Section 809. Parental bereavement leave

Section 809 amends Title 5, Section 6329d to extend bereavement leave to employees who have suffered the natural or spontaneous loss of an unborn child.

Section 810. Definition of foreign instrumentality for purposes of economic espionage prohibition

Section 810 amends the definition of foreign instrumentalities in Title 18, Section 1839 to include enterprises domiciled in Russia, China, Iran, or the DPRK.

Section 811. Protection of trade secrets

Section 811 amends Title 18 to extend jurisdiction over economic espionage and theft of trade secret offenses, criminalize the unauthorized transmission of trade secrets outside the United States, criminalize inciting the theft of trade secrets and economic espionage, and establish that enterprises domiciled in Russia, China, Iran, or the DPRK are foreign instrumentalities for the purposes of the chapter.

Section 812. Technical amendments

Section 812 makes minor technical amendments to the *National Security Act of 1947*.

COMMITTEE COMMENTS AND DIRECTION

Notification of Certain Declassifications

The Committee has historically not received timely notice when the heads of IC elements declassify or downgrade information or intelligence relating to intelligence sources, methods, or activities. Therefore, the Committee directs the DNI, or the Principal Deputy DNI, as delegated by the DNI, to notify the congressional intelligence committees and the Archivist of the United States in writing immediately upon declassifying, downgrading, or directing the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities pursuant to section 3.1(c) of Executive Order 13526, or any successor order. The Committee further directs the head, or senior official, of each element of the IC, to notify the congressional intelligence committees and the Archivist of the United States in writing immediately upon declassifying, downgrading, or directing the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities pursuant to section 3.1(d) of Executive Order 13526, or any successor order. Each notification made pursuant to this paragraph shall include a copy of the information that has been, or has been directed to be, declassified or downgraded.

Briefing on Space and Counterspace Matters

The Committee derives enormous value from ad hoc, periodic briefings from both the Department of Defense (DoD) and IC on combined Title 10 and Title 50 activity in the space domain. The Committee particularly values the congressional defense committees endorsement of one-time read-ins for select Title 10 programs to enhance the congressional intelligence committees' understanding of how the DoD defends the IC space architecture. However, the Committee remains concerned about siloes between Title 10 and Title 50 special access programs that impede oversight.

Therefore, the Committee will continue its practice of holding an annual briefing with the Director of the NRO and the Chief of Space Operations of the Space Force. This briefing shall include (1) an assessment of the space and counterspace capabilities of the United States and its adversaries; (2) an identification of all threats to the national security space infrastructure of the United States; and (3) proposals of any policy needed to protect, or otherwise advance, the national security interests of the United States in space. Each briefing shall be conducted at the highest classification level without restrictions, and all compartmented information related to space and counterspace matters shall be made available to the Committee during the briefing.

Requirement for Office of the Director of National Intelligence to Establish a Memorandum of Understanding with the National Defense University Clarifying its Role in the National Intelligence University

The Committee supports the decision of the DNI to transfer responsibility for the NIU to the NDU. However, there remain many unanswered questions about what role, if any, the DNI will play in providing financial resources for NIU infrastructure, students, staff and faculty, or research efforts; allowing NIU students to continue using Roberdeau Hall during the transfer period; participating in the Senior Advisory Board to provide strategic direction and input into NIU's curriculum; and ensuring that ODNI students, faculty, or staff may participate in the NIU once it has transferred to NDU. Therefore, the Committee directs the DNI to establish a Memorandum of Understanding with NDU within 90 days of enactment of this Act that addresses these questions and any other issues that the President of NDU deems necessary to ensure a successful transfer of NIU.

Declassification of Church Committee Archival Records

Per the stipulations in S. Res. 474 (96th Cong.), the archival records of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("the Church Committee") become eligible for public release starting in October 2026 after undergoing a declassification review. This Committee supports the expeditious public release of these historically valuable records and directs CIA to prioritize their declassification. Furthermore, this Committee supports CIA's usage of appropriate AI tools to expedite the declassification process.

Countering Foreign Malicious Cybercriminal Organizations

The Committee directs that, not later than 180 days after the date of the enactment of this Act, the DNI, in consultation with the Director of the FBI, shall submit to the Committee a report on hostile foreign cyber actors, such as foreign scam centers and including, at a minimum, Prince Group, Huione Group, L.Y.P. Group, Jin Bei Group, Funnull Technology Inc., TransAsia International Holding Group Thailand Company Limited, The Democratic Karen Benevolent Army, and HH Bank Cambodia PLC. The report should include:

(A) An identification of the individuals and entities constituting hostile foreign cyber actors, including foreign scam centers, that pose the most significant threat.

(B) An identification of the locations from which the individuals and entities identified under subparagraph (A) operate.

(C) A description of the infrastructure, tactics, and techniques hostile foreign cyber actors, including foreign scam centers, commonly use, including reliance on any products or services subject to the jurisdiction of the United States.

(D) A description of any relationships between the individuals and entities that operate hostile foreign cyber actors, including foreign scam centers, and their governments or countries of origin that could impede the ability to counter threats from such centers.

(E) An identification of communications and financial services providers subject to the jurisdiction of the United States that provide enabling services to individuals and entities identified under subparagraph (A).

(F) A description of any relationships that the individuals and entities identified under subparagraph (A) have with transnational organized crime groups.

(G) A discussion of the relationships, if any, between foreign hostile foreign cyber actors, including scam centers, and foreign security services.

(H) A discussion of any intelligence collection gaps on such hostile foreign cyber actors, including scam centers.

(I) A description of the available authorities across the IC to disrupt the activities of these centers which target U.S. persons.

The report shall be submitted in unclassified form, but may include a classified annex. The unclassified form of the report shall be made available to the public.

Prohibition on Clearance Holder Participation in Online Prediction Markets

Not later than 45 days after the date of the enactment of this Act, the DNI shall issue a policy restricting the participation of covered individuals in online prediction markets. "Covered individual" means an employee or contractor, or a former employee or contractor, of an element of the IC who holds a security clearance. The policy shall provide that, except as necessary to conduct authorized intelligence activities, no covered individual may participate in any online prediction market (including any online platform that allows agreements, contracts, transactions, or swaps between users over the outcome of non-financial future events, such as sports, military

activities, and elections) on any topic relating to nonpublic information to which the covered individual has or had access by virtue of being a covered individual. The prohibition shall be in effect during (a) the period during which the covered individual is employed or contracted by an element of the IC and (b) the two-year period beginning on the date on which the covered individual ceases to be employed or contracted by an element of the IC. The policy shall establish appropriate penalties for violating the prohibition and providing notice to all covered individuals.

National Counterterrorism Center Social Media Report

The Committee directs that, not later than 120 days after the date of the enactment of this Act, the NCTC shall submit a classified report to the Committee identifying existing challenges for the counterterrorism enterprise in removing foreign terrorism recruitment content on each widely used social media platform where online radicalization takes place. Such a report should detail any current legal restrictions and social media platform policies which prevent content removal.

IC Efforts Against PRC Cislunar Ambitions

The Committee believes that the United States has real and growing political, economic, and strategic interests in cislunar space. Meanwhile, the PRC is moving aggressively to promote its interests in cislunar space, at the expense of the United States and the friends and allies of the United States. The Committee believes the IC must increase its focus on PRC cislunar programs, activities, and intentions. Therefore, the Committee directs the DNI to prepare and submit to the Committee a report that addresses the following matters: an assessment of the current IC posture to collect timely and actionable intelligence and provide insightful analysis on the PRC's cislunar plans, capabilities and operations; a plan to significantly enhance the IC's posture both in terms of personnel and collection capabilities to collect information and provide timely analysis of the PRC's cislunar space plans, capabilities, and operations; and a listing of the funding required, on an annual basis over the next five years, to implement such a plan, including the recommended allocation of funds across the various IC organizations.

The Committee also directs the DNI to establish an information exchange program to facilitate engagement with U.S. companies that are involved in developing, deploying and operating cislunar and lunar space systems. Such engagements should include information sharing regarding the PRC's cislunar space plans, capabilities and operations.

Strategy on Intelligence Sharing and Briefings for Artificial Intelligence Vendors and Researchers

The Committee has closely tracked the extent to which leading AI systems demonstrate advanced capabilities in the generation of synthetic media and computer programming code, and in areas such as object recognition, natural language processing, complex system design, and workflow orchestration. These advanced capabilities, and their accessibility to a wide range of users, have increased the rate of development and adoption by foreign adversary

countries, which have used or illicitly acquired American AI capabilities to generate synthetic media for influence campaigns, develop and manage computer network exploitation campaigns, design or develop weapons systems, enhance surveillance capabilities in ways that undermine the privacy and threaten the security of citizens of the United States, and facilitate illicit technology transfer.

The Committee believes that the provision of expedited clearance adjudication, or one-time read-ins, for leading AI vendors and researchers would dramatically enhance the ability of the United States to identify and counter threats posed by foreign adversary countries enabled by, or directed toward, commercial AI capabilities in the United States. Additionally, the Committee has repeatedly heard that a gap exists in engaging leading U.S. AI firms and researchers with respect to counterintelligence risks posed by foreign adversary use or targeting of AI capabilities of U.S. providers.

Therefore, the Committee directs the Director of the National Counterintelligence and Security Center (NCSC) and the Assistant Director of the FBI for the Counterintelligence Division to jointly establish and implement a strategy to provide threat intelligence, defensive briefings, and bidirectional information exchanges, as appropriate, for vendors of AI systems, including model developers and infrastructure providers, and other relevant entities and individuals, such as academic or nonprofit researchers, and to solicit voluntarily, as appropriate and consistent with applicable laws, information from such vendors and other relevant entities and individuals regarding:

(A) Efforts by foreign adversary countries to use products or research of such vendors or other entities or individuals for malicious activity described above.

(B) Threats posed by foreign adversary countries, including indications of compromise to networks associated with such vendors and other entities and individuals, or other technical indicators, indicating a compromise to the confidentiality, integrity, or availability of an AI system, or to the supply chain of an AI system, including training or test data, frameworks or software libraries, training or inference computing environments, or other components necessary for the training, management, or maintenance of an AI system.

(C) Activity of foreign entities of concern to clandestinely, fraudulently, or otherwise maliciously access the systems of such vendors for purposes of illicit technology transfer or otherwise gaining unfair economic advantage, including through techniques to extract a model's technical capabilities to replicate, develop, or improve a foreign AI model without authorization by the vendor.

(D) Activity of foreign entities of concern to sabotage or otherwise clandestinely degrade AI systems or the supply chain of an AI system, including training or test data, frameworks or software libraries, training or inference computing environments, or other components necessary for the training, management, or maintenance of an AI system.

(E) Observations, emerging concerns, or other inputs from vendors or researchers regarding relevant malicious or clandes-

tine activity of foreign entities of concern toward an AI system, its supply chain, or other necessary components.

To the greatest extent practicable, the Committee encourages such a strategy to leverage existing information sharing processes, including those that protect sensitive information shared from private sector parties from disclosure and provide legal protections for sharing information with the U.S. Government.

Implementation of Comptroller General Recommendations Relating to the Personnel Security Clearance Process

While the timeliness of security clearances related to onboarding has improved, the data needed to analyze choke points, costs, and reciprocity issues for purposes of cost efficiencies and overall improvement of the security clearance process is vital. The Committee notes that the Government Accountability Office (GAO) published several reports on the government-wide personnel security clearance process, including recommendations to the DNI. The Committee is encouraged that ODNI implemented many of these recommendations and made progress resolving issues GAO identified. Still, more work remains as ODNI has not fully implemented all of GAO's recommendations on this process.

In particular, the Committee shares the concerns highlighted in GAO–26–107100, "Personnel Security Clearances: Actions Needed to Address Significant Data Reliability Issues That Impact Oversight," dated December 11, 2025, regarding the DNI's oversight of agencies' security clearance processes, particularly regarding the data ODNI collects from agencies on timeliness, the number of investigations completed, and other key aspects of the personnel security process. The Committee also shares GAO's concerns that ODNI has not issued adequate guidance to agencies for assessing their data and does not review the data it collects in a way that aligns with data reliability principles.

Thus, the Committee agrees that the DNI should promptly take the following actions to implement GAO's recommendations in that report:

(A) Develop and implement a process that guides ODNI's efforts to assess agencies' security clearance data. This process should incorporate data reliability practices or principles, such as those found in GAO's "Assessing Data Reliability" (GAO–20–283G), dated December 16, 2019, or those established by Data Management Association International in chapter 13 of its "DAMA–DMBOK: Data Management Body of Knowledge," 2nd edition, 2017.

(B) Issue and monitor agencies' adherence to guidance clarifying the agencies' role in assessing data to improve the reliability of the data they report to ODNI. The guidance should require agencies to assess the characteristics, quality controls, and limitations of their data, using data reliability practices or principles, and address any gaps.

(C) Define, at each relevant agency, the senior data official's role for assessing the reliability of the agency's data, and ensure agencies have identified these accountable officials.

(D) Analyze and update, to the maximum extent practicable, ODNI's personnel vetting policy framework to incorporate GAO's key practices for evidence-building and performance-

management activities from its report "Evidence-Based Policymaking: Practices to Help Manage and Assess the Results of Federal Efforts" (GAO–23–105460), dated July 12, 2023, and apply those practices in its oversight of the clearance process.

Audit of Intelligence Support to the National Vetting Center

The Committee remains concerned by efforts of the PRC to access, surveil, and potentially disrupt or steal sensitive academic research within the United States. The National Vetting Center (NVC) and the companion Intelligence Community Support Element (ICSE) play an important role in supporting the vetting of visa applications by foreign nationals, including those seeking access to institutes of higher education engaging in sensitive research, including defense- and national security-related research. However, the Committee is concerned about the level of IC support to the NVC and supports efforts to protect against espionage and the illicit transfer of critical and emerging technologies to countries of concern.

Therefore, the Committee directs the Comptroller General of the United States to conduct a performance audit of the ICSE's role in supporting vetting of applications for student and research visas by PRC nationals.

The Committee further directs the Comptroller General to brief the Committee on its review within 180 days, with final results to follow in a mutually agreed upon timeframe and format.

Exploiting Commercial Hypersonic Capabilities for Indications & Warning Validation

The Committee notes the rapid pace at which adversary hypersonic capabilities—including the People's Liberation Army (PLA) Air Force's fielding of fighter-launched hypersonic missiles, the PLA Rocket Force's continued expansion of hypersonic glide vehicle inventories, and Russian deployment of multiple maneuverable hypersonic systems—are challenging the IC's ability to characterize and identify indicators and warnings and counter these threats at the pace of fielding.

The Committee further notes that the United States benefits from a uniquely competitive commercial hypersonic flight test ecosystem, with multiple providers conducting recurring flight test campaigns at scale. The Committee believes that this domestic ecosystem represents an underutilized resource for IC foreign hypersonic threat exploitation activities, including signature characterization, sensor calibration, indication-and-warning algorithm development, and red-team threat representation for IC test and evaluation events.

The Committee therefore directs the DNI, in coordination with the Under Secretary of Defense for Intelligence and Security and the Director of the Defense Intelligence Agency, to conduct an assessment of opportunities for the IC to leverage U.S. commercial hypersonic flight test capabilities—particularly those capable of air-launched, multi-salvo, and rapidly reconfigurable threat-representative profiles—to accelerate foreign hypersonic threat understanding, sensor calibration, and indications-and-warning system development. The assessment shall be provided to the congressional intelligence committees not later than 180 days after the en-

actment of this Act, and shall include any required authorities, funding mechanisms, or interagency arrangements necessary to formalize IC use of commercial hypersonic flight test capabilities as a sustained intelligence enterprise activity.

Voice-based Risk Assessment Tools

The Committee recognizes the ongoing importance and increasing challenge of properly vetting individuals who will be granted access to sensitive installations throughout the U.S. national security enterprise. Validating assets, vetting foreign nationals and supply chain partners, and conducting continuous evaluation for existing personnel and contractors all place restraints on capacity and resources that limit the speed and scale of action across the national security workforce and its supporting industrial base.

As the IC continues to look for ways to address these challenges, the Committee encourages the elements of the IC to evaluate emerging technologies, including voice-based risk assessment tools, that offer the potential to augment and complement human-led investigative and vetting processes, reduce backlogs, support faster and more scalable adjudications, and strengthen screening of assets, personnel, contractors, vendors, and other third parties with access to sensitive programs, facilities, or information. While such technologies may not be a perfect fit for every agency, it is critical to explore the use of all tools that can mitigate counterintelligence risks to the national security enterprise.

Synchronizing National Reconnaissance Office and National Geospatial-Intelligence Agency Efforts Related to Commercial Imagery Acquisition

The NRO is the primary acquirer of commercial satellite imagery for the IC and the DoD, while the National Geospatial-Intelligence Agency (NGA) is responsible for fulfilling geospatial intelligence (GEOINT) requirements of the IC and DoD, in addition to its responsibility for acquiring commercial GEOINT analytic services, or value-added imagery products. NRO's Electro-Optical Commercial Layer (EOCL) contract is based on NGA's validated GEOINT requirements to meet IC and DoD commercial imagery needs through 2032.

The Committee has long been concerned about low levels of funding for commercial imagery and has questioned whether the EOCL contract is flexible enough to keep up with emerging commercial imagery capabilities and constellations. The Committee has also been concerned that NRO's acquisition of commercial imagery under the EOCL contract is not well aligned to NGA's validated GEOINT requirements, resulting in contracting, resourcing, and management tensions between NRO and NGA and shortfalls in the collection of foundation GEOINT imagery.

The Committee maintains that deeper integration of the NRO and NGA commercial offices can help both organizations address longstanding challenges to their ability to fully address IC and DoD commercial imagery needs. The Committee therefore directs the Directors of the NGA and the NRO to jointly develop and submit to the Committee quarterly progress reports through fiscal year 2027—aligned to the delivery of existing quarterly commercial imagery updates—on efforts to synchronize ongoing agency efforts re-

lated to commercial imagery acquisition. Those efforts include: (1) further integration of the NRO and NGA commercial offices through processes, documentation, activities, and personnel exchanges; (2) improving alignment of commercial imagery contracts to validated foundation imagery requirements; and (3) determining the best approach to integrate commercial imagery data into the ground system architecture in a manner that ensures flexibility and traceability of requirements.

Intelligence Diplomacy

The Committee recognizes that intelligence diplomacy—defined by Intelligence Community Directive 405 (ICD–405) as the sharing of intelligence information with a foreign government on a specific threat or issue in support of a preferred policy objective—is critical to advancing U.S. foreign policy and national security goals. The Committee recognizes that intelligence diplomacy provides unique mechanisms for advancing U.S. strategic objectives through structured engagement with foreign partners, as well as a vehicle for ally and partner capacity-building through technical assistance, professional development, and infrastructure modernization. Collectively, these and related efforts help build institutional trust and generate enduring decision advantage for the United States and its partners.

Accordingly, the Committee supports elevating intelligence diplomacy as a tool of U.S. statecraft and directs the DNI, in coordination with the Secretary of Defense and the heads of relevant IC elements, to prioritize sustained investment in intelligence diplomacy initiatives with Major Non-NATO Allies and other key partner nations. Such initiatives should include institutional capacity-building, partner professionalization, senior leader engagement, robust bilateral intelligence exchanges, tailored liaison officer exchanges, and the development of bilateral intelligence-sharing agreements. These efforts should advance U.S. strategic interests, counter adversary influence and gray-zone activities, and bolster allied resilience against current and future security challenges.

Proliferation Assessments Regarding the Export of Artificial Intelligence-Related Technologies

The Committee believes that proliferation of advanced AI technology presents a unique national security challenge. Frontier AI systems—including the most capable model weights, advanced integrated circuits, and the manufacturing equipment required to produce them—can be leveraged by U.S. adversaries for applications ranging from autonomous weapons and signals intelligence exploitation to mass surveillance and offensive cyber operations. A single export decision that places these capabilities in the hands of a U.S. adversary could degrade U.S. military and intelligence advantages for years, particularly if the technology is subject to onward transfer to adversary end-users beyond the reach of U.S. enforcement.

The Committee is unaware of any formal mechanism to ensure that a comprehensive national security assessment reaches the President and Congress before a consequential export is approved. Meanwhile, Congress has mandated intelligence assessments in analogous high-stakes export contexts. The Committee finds that

the strategic importance of advanced AI technology—and the difficulty of reversing the consequences of a flawed export decision—warrants a comparable mechanism.

Accordingly, the DNI, acting through the National Intelligence Council and in coordination with the Directors of the CIA and the NSA, and the heads of other appropriate elements of the IC, is directed to produce a written report for the President and the congressional intelligence committees no fewer than 90 days before either (1) the Secretary of Commerce grants a license for the export, reexport, or in-country transfer of AI intelligence technology—including U.S.-origin model weights, advanced integrated circuits, semiconductor manufacturing equipment, and items controlled under ECCN 3A090 or 4A090; or (2) the United States enters into or joins an agreement on AI with a foreign government.

The report should include the following information:

(A) An assessment of recipient country's export control system for AI technology.

(B) Past, present, or expected commercial and governmental interactions between the recipient and countries of proliferation concern, particularly China.

(C) An assessment of the consequences of onward proliferation for U.S. national security.

(D) Mitigation measures the recipient could reasonably undertake.

(E) In the case of a license, specific IC measures to evaluate compliance with associated restrictions.

(F) Whether the recipient's intended and likely end uses, including military, intelligence, and surveillance applications, are consistent with U.S. national security interests.

Each report should be submitted in unclassified form, but may include a classified annex.

Prohibition on NCTC Assessments with No Foreign Nexus

The Committee directs that no funds authorized to be appropriated by this Act may be used by the NCTC to prepare or contribute to intelligence analytic products concerning terrorist threats that have no identified foreign nexus. This direction shall not be interpreted as restricting the Director of NCTC from responding to a terrorist attack of unknown origin that takes place in the United States or from performing activities necessary to determine determining whether an individual or group operating within the United States has any connection to a known or suspected foreign terrorist, foreign terrorist group, foreign power, or other foreign entity.

Prohibition on Use of National Intelligence Program Funds for Domestic Terrorism Analysis by the Department of Homeland Security Office of Intelligence and Analysis

The Committee is concerned about the use of NIP funds to collect information on U.S. persons absent any affiliation with foreign intelligence or foreign adversaries, and the subsequent dissemination and/or use of that information. Therefore, the Committee directs that no funds authorized to be appropriated by this Act may be used by the DHS I&A for purposes of domestic terrorism analysis. This direction shall not be interpreted as restricting I&A from re-

sponding to a terrorist attack of unknown origin that takes place inside the United States or from performing activities necessary to determine whether a violent extremist or group operating within the United States has any connections to a known or suspected foreign terrorist, foreign terrorist group, foreign power, or other foreign entity.

Russia and China Nuclear Tests

The Committee appreciates the IC keeping the Committee fully and currently informed of the nuclear developments of Russia and China.

Since signing the Comprehensive Nuclear Test Ban Treaty (CTBT) in 1996, China and Russia have conducted yield-producing nuclear weapons tests. Both China and Russia have built extensive nuclear test ranges in underground facilities and have taken steps to avoid their test activities being detected by the International Monitoring System (IMS).

China conducted annual nuclear-weapons-related tests at its Lop Nur nuclear test site in support of its nuclear expansion efforts. Some of these tests were intended to produce yields up to hundreds of tons. An IMS seismic station in Kazakhstan detected one of China's tests on 22 June 2020. During the last few years, China has expanded many facilities at Lop Nur, illustrating continued support for its testing activities and suggesting that designers will execute more complex test seasons in the future.

Russia has conducted annual nuclear-weapons-related tests at its Novaya Zemlya nuclear test facility every year, except for 2020. Some of these tests have produced nuclear yield that would be inconsistent with the US's interpretation of zero-yield CTBT.

Access to Classified Intelligence Information Outside of Established Review Processes

The Committee directs that, not later than 120 days after the date of the enactment of the Act, and annually thereafter for 5 years, the DNI shall submit to the congressional intelligence committees a report on the approval of interim security clearances, or other approvals to access classified intelligence information that deviate from the investigative and adjudicative standards established under Executive Order 12968 (50 U.S.C. § 3161 note; relating to access to classified information), for employees or contractors of the IC, or other individuals granted access to the facilities or information maintained by the IC, during the preceding calendar year.

The Committee directs that the first report under this provision shall include information for each of the calendar years 2017 through 2026. Each report required by this provision should include: (1) the number of such approvals, disaggregated by sponsoring agency, duration of access, and level of security clearance or access; (2) the investigative and adjudicative process conducted, if any, for each such level of security clearance or access; (3) a categorization of the justifications supporting such approvals, and the number of approvals in each category; and (4) the disposition of such approvals after 6 months from the initial access or interim clearance, disaggregated by the number of instances in which access was terminated, continued, or resulted in completion of a proc-

ess satisfying investigative and adjudicative standards required by Executive Order 12986.

COMMITTEE ACTION

On May 20, 2026, 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

The Committee made the Chairman's and Vice Chairman's bill, together with the classified annex for Fiscal Year 2027, the base text for purposes of amendment.

By voice vote, the Committee adopted *en bloc* twenty-two amendments to the base text.

By a vote of 8 ayes and 9 noes, the Committee did not adopt an amendment by Senator Wyden to amend the *National Security Act of 1947* and the *Intelligence Reform and Terrorism Prevention Act of 2004* regarding certain whistleblower-related authorities. The votes in person or by proxy were as follows: Chairman Cotton—no; Senator Risch—no; Senator Collins—no; Senator Cornyn—no; Senator Moran—no; Senator Lankford—no; Senator Rounds—no; Senator Young—no; Senator Budd—no; Vice Chairman Warner—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Bennet—aye; Senator Gillibrand—aye; Senator Ossoff—aye; Senator Kelly—aye.

By a vote of 8 ayes and 9 noes, the Committee did not adopt an amendment by Senator Wyden to prohibit IC contractors and subcontractors from collecting and selling certain location data. The votes in person or by proxy were as follows: Chairman Cotton—no; Senator Risch—no; Senator Collins—no; Senator Cornyn—no; Senator Moran—no; Senator Lankford—no; Senator Rounds—no; Senator Young—no; Senator Budd—no; Vice Chairman Warner—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Bennet—aye; Senator Gillibrand—aye; Senator Ossoff—aye; Senator Kelly—aye.

By a vote of 9 ayes and 8 noes, the Committee adopted a motion to table by Chairman Cotton in response to Senator Wyden's appeal of the ruling of the Chairman that Senator Wyden's two annex amendments were not filed in compliance with Committee deadlines. The votes in person or by proxy were as follows: Chairman Cotton—aye; Senator Risch—aye; Senator Collins—aye; Senator Cornyn—aye; Senator Moran—aye; Senator Lankford—aye; Senator Rounds—aye; Senator Young—aye; Senator Budd—aye; Vice Chairman Warner—no; Senator Wyden—no; Senator Heinrich—no; Senator King—no; Senator Bennet—no; Senator Gillibrand—no; Senator Ossoff—no; Senator Kelly—no.

Votes to report the committee bill

On May 20, 2026, the Committee voted to report the bill, as amended, by a vote of 14 ayes and 3 noes. The votes in person or by proxy were as follows: Chairman Cotton—aye; Senator Risch—aye; Senator Collins—aye; Senator Cornyn—aye; Senator Moran—aye; Senator Lankford—aye; Senator Rounds—aye; Senator Young—aye; Senator Budd—aye; Vice Chairman Warner—aye; Senator Wyden—no; Senator Heinrich—no; Senator King—aye;

Senator Bennet—aye; Senator Gillibrand—aye; Senator Ossoff—no; Senator Kelly—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 20, 2026, 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.

ADDITIONAL VIEWS OF CHAIRMAN COTTON, SENATOR RISCH, SENATOR COLLINS, SENATOR ROUNDS, AND SENATOR BUDD

We are pleased to include in this bill several corrective provisions that respond to abuses of intelligence authorities that took place under the Biden administration. First, this bill clarifies that the definition of intelligence includes *only* foreign intelligence and counterintelligence. According to 50 U.S.C. § 3003, "the term 'intelligence includes 'foreign intelligence' and 'counterintelligence'." Yet under the Biden administration, we witnessed various elements of the Intelligence Community (IC) engage in mission creep into purely domestic activities. Section 609 of the bill refines the definition of intelligence to ensure only foreign and counterintelligence can be considered as "intelligence" for the purposes of intelligence activities under Title 50.

Similarly, the National Counterterrorism Center (NCTC) under the Biden administration interpreted the existing statute as permitting the production of intelligence analysis on domestic, law enforcement matters lacking any foreign or counterintelligence nexus. The NCTC was established by the *Intelligence Reform and Terrorism Prevention Act of 2004* (P.L. 108–458) in response to the failure of law enforcement and the IC to "connect the dots" leading up to the September 11, 2001 attacks. The NCTC was to serve as a "go-between" where law enforcement could check IC holdings as to whether a person of interest in a terrorism investigation might have a connection to foreign terrorist groups. The NCTC itself was never meant to work solely in the domestic, law enforcement space. Section 305 of the bill clarifies a limitation in what NCTC can do with regard to domestic activities. While it remains entirely appropriate for law enforcement to query NCTC's holdings for foreign connections, NCTC may not perform solely domestic work. Nothing in this section is meant to limit NCTC's support for Trump administration efforts to go after transnational criminal organizations such as the cartels, all of which have been designated as "foreign terrorist organizations" and therefore fall squarely within NCTC's responsibilities.

The Office of Intelligence and Analysis (I&A) at the Department of Homeland Security (DHS) was established in 2002 with the enactment of the *Homeland Security Act* (P.L. 107–296). Its primary mission was to "access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information" in order to identify, assess, detect, and understand terrorist threats to the homeland. This mission filled a critical gap by enabling information sharing among state and local governments, the private sector, and relevant parts

of the Federal government (including the IC and the other components of DHS). This was in keeping with the long-held precedent in U.S. law that foreign intelligence collection and analysis should be separate and distinct from domestic law enforcement.

With enactment in 2007 of the *Implementing Recommendations of the 9/11 Commission Act* (P.L. 110–53), I&A's mission expanded beyond facilitating information sharing to preventing terror attacks against the homeland. Specifically, this Act directed I&A to support both the functions of the newly-created National Counterterrorism Center, as well as the *"mission responsibilities of the Department"* as they related to terrorism against the homeland. This is significant, because DHS defines "terrorism" in part as "any activity that involves *an act that is dangerous to human life* or potentially destructive of critical infrastructure or key resources, and *is a violation of the criminal laws* of the United States or of any State or other subdivision of the United States." This statute fundamentally changed I&A's original foreign intelligence function by giving it responsibilities that fall squarely in the domestic, law enforcement arena.

The Committee has witnessed this statute being used inappropriately in numerous instances, to include in 2021, when I&A began producing analysis on "domestic terrorism" that lacked any connection to a foreign nexus. It was also deputized to be a part of DHS's ill-advised, and now-defunct, "Disinformation Governance Board," an effort to restrict American speech by labeling speech the government disapproved of as "disinformation." I&A also collects information on U.S. persons, even if those individuals lack any foreign or counterintelligence nexus. These are just some of the disturbing activities I&A supported in recent years.

Intelligence elements should not engage in activities that lack any foreign intelligence or counterintelligence nexus, and we are pleased that the underlying bill includes a section that provides needed reforms to I&A.

Section 506 amends I&A's underlying statute to ensure that it stays within the scope of responsibilities of an intelligence element. Specifically, section 506 replaces the references to "terrorism" or "terror attacks" with "foreign threats," and strikes I&A's responsibility to support the "mission responsibilities of the Department." Further, section 506 better protects Americans' privacy by prohibiting I&A from collecting any intelligence or information on U.S. persons, and prohibiting any clandestine collection.

The IC is vitally important to national security, and it is critical that it remain laser-focused on foreign intelligence threats to the United States. Domestic activities lacking any foreign intelligence nexus fall squarely within law enforcement. We are pleased that several of the provisions in the Intelligence Authorization Act for Fiscal Year 2027 reinforce this important distinction.

With enactment of the *Intelligence Reform and Terrorism Prevention Act of 2004* (P.L. 108–458), Congress provided the Director of National Intelligence (DNI) broad authority to coordinate relationships and intelligence sharing with foreign intelligence services with the expectation that the DNI would be transparent with the congressional intelligence committees in doing so. At the time, Congress did not believe it was necessary to hold the DNI to the same

notification requirements imposed on the Secretaries of Defense and State for military assistance. However, during Israel's effort to bring to justice the HAMAS perpetrators of the horrific October 7, 2023 attacks on Israeli civilians as well as hostage recovery efforts of United States persons, the Secretary of Defense notified Congress of pauses in weapons shipments, but DNI Avril Haines did not notify Congress regarding any adjustments to intelligence support to Israel. This lack of transparency hinders the congressional intelligence committees' oversight responsibilities to ensure that intelligence sharing enhances the bilateral relationship between Israel and the United States.

Section 622 amends the DNI's authority to require notification to the congressional intelligence committees of any major change to the intelligence sharing relationship between the United States and Israel and prohibits suspension or material reduction of intelligence sharing with Israel absent a significant national security concern. It further authorizes DNI Walter "Jay" Clayton and the Trump administration to enhance intelligence sharing with Israel and Abraham Accord countries in support of the President's policies to eliminate the threat posed by Iran.

TOM COTTON.
JAMES E. RISCH.
SUSAN M. COLLINS.
M. MICHAEL ROUNDS.
TED BUDD.

ADDITIONAL VIEWS OF SENATOR BENNET

I am pleased that under the leadership of Chairman Cotton and Vice Chairman Warner, the Committee reached bipartisan agreement on an Intelligence Authorization Act (IAA) for Fiscal Year 2027 that will strengthen U.S. national security by providing our intelligence community (IC) personnel, including thousands of Coloradans, with the resources and authorities that they need to protect our nation.

This bill addresses many of my priorities, most especially the importance of ensuring the uninterrupted provision of U.S. intelligence support to Ukraine. As a result of U.S. and allied investments, Ukraine has substantially halted Russia's momentum on the battlefield and developed a capacity to conduct warfare unlike any NATO member state. Ukraine's armed forces are now not only less dependent on U.S. military support; they also are postured to contribute to U.S. and NATO efforts to deter and help defeat any future Russian aggression in Europe, as well as address evolving threats to U.S. forces in the Middle East and Indo-Pacific.

The Committee's bipartisan action to codify U.S. intelligence support to Ukraine in this bill ensures that the architecture underlying Ukraine's recent battlefield success will not be interrupted and increases pressure on Russian President Putin to come to the negotiating table, supporting diplomacy aimed at securing a comprehensive settlement of the conflict. Moreover, by removing the ambiguity as to whether the United States will continue its intelligence support of Ukraine in the event of any future peace deal, the bill enables long-term planning, budgeting, and execution by the IC necessary to help enforce a future agreement, bolster U.S. and NATO deterrence against future Russian aggression, and deepen joint efforts with Ukraine in areas of mutual benefit (e.g., U.S.-Ukraine cooperation on unmanned aerial systems and countering unmanned aerial systems, which Sen. McConnell and I propose to strengthen through the Fiscal Year 2027 National Defense Authorization Act).

I am similarly pleased that this bill provides for stronger intelligence cooperation with U.S. allies and partners in the Indo-Pacific to enhance multilateral deterrence, requires measures to address the national security risks posed by the proliferation of artificial intelligence (AI) technologies to U.S. adversaries, and supports sustained investment in intelligence diplomacy. These are all priorities that I championed.

Separately, and consistent with the Committee's longstanding practice, the bill provides for continued U.S. intelligence cooperation with Israel. Although such cooperation offers potential benefits to the United States, I am concerned by the gaps between what Israeli intelligence officials reportedly anticipated would occur in the event of an armed conflict with Iran and what has unfolded

after the United States and Israel jointly attacked Iran on February 28, 2026, without congressional authorization. Additional bipartisan oversight is necessary to clarify why senior U.S. decision-makers apparently discounted U.S. intelligence and military assessments that diverged from Israel's optimistic—and, in hindsight, mostly inaccurate—projections of how the war with Iran would unfold.

I have repeatedly warned that some actions by Prime Minister Netanyahu's government are detrimental to U.S. national security and risk undermining the American people's support for U.S.-Israel security cooperation. In particular, I am gravely concerned by the explosion in extremist settler violence in the West Bank, which affects U.S. citizens and permanent residents and which current and former Israeli officials acknowledge the Netanyahu government has failed to curtail. As I noted during the drafting process of this year's IAA, the U.S. government lacks a systematic intelligence assessment of extremist settler violence in the West Bank and the consequences for U.S. policy goals. I hope there will be bipartisan support in the future for directing the production of such an assessment, consistent with Congress's Article I authority to direct intelligence production in support of its oversight responsibilities.

Similarly, senior Administration officials, including the President, Vice President, and Secretary of State, have rightly and publicly reaffirmed U.S. opposition to Israeli annexation of the West Bank. In seeming contravention of this U.S. policy, however, the Netanyahu government has directed record levels of new settlement authorization in the West Bank, legalized previously unauthorized outposts, approved large-scale land declarations, and provided for significant Israeli government expenditures on settlement construction and administration. Structured IC scrutiny of these and other Israeli activities, in the form of a recurring assessment, would inform Congress' oversight.

I have long argued that the IC is the essential backbone of U.S. national security. Critical to the IC's remarkable successes is ensuring that our IC personnel are not asked to undertake missions that may be better suited for other U.S. departments and agencies. Indeed, experience suggests that IC mission creep and an over-reliance by policymakers on covert tools of statecraft can sometimes lead to unintended consequences and undermine progress toward U.S. national security goals. With this as context, I expect that the Committee, in furtherance of its best bipartisan tradition and mandate, will continue robust oversight aimed at ensuring that the IC's evolving activities and mission set complement and do not supplant the equally consequential work performed by U.S. diplomats and military personnel.

MICHAEL F. BENNET.

MINORITY VIEWS OF SENATOR WYDEN

The Fiscal Year 2027 Intelligence Authorization Act represents a dramatic retreat from years, and in some cases decades, of congressional oversight.

As was the case last year, the bill eliminates Senate Advice and Consent for key Intelligence Community leadership positions. First, it surrenders the Committee's, and the Senate's, opportunity to vet the general counsels of the CIA and the Office of the Director of National Intelligence. At a time of rampant lawbreaking by the Trump Administration, it is especially troubling that the only Intelligence Community general counsels currently subject to Senate confirmation—the people responsible for offering legal advice on secret, potentially controversial intelligence activities—would be appointed without any congressional or public input or scrutiny.

The bill also eliminates Senate Advice and Consent for the Director of the National Counterterrorism Center at a time in which the Center is expanding its activities into the realm of domestic law enforcement, particularly through the NCTC Intelligence Fusion Center, in a manner that poses a real danger to Americans' rights. It also removes the Director of the National Counterintelligence and Security Center from the Senate confirmation process, even as the bill puts the Director in charge of a new Intelligence Community Counterintelligence Office in the Department of Commerce, a wrongheaded and unnecessary expansion of the Intelligence Community.

This year's bill omits important whistleblower protections that have been in previous Committee-reported bills, in some cases for the last five years. I am disappointed that my amendment to include these whistleblower protections in the bill was defeated on a party-line vote. The Committee's retreat from what had been a long-standing bipartisan approach to whistleblower protection legislation is especially troubling during an administration that commits so many abuses. I do welcome a provision preventing the DNI and the CIA Director from thwarting whistleblowers' efforts to come to Congress by denying them guidance on how to do so, a problem I have long sought to address. The bill does not, however, resolve the legitimate concerns of whistleblowers who may not want the details of their complaints submitted to the directors in the first place, for fear of retaliation.

The bill also excludes a critically important provision that was included in last year's bill. That provision stated that, if a company wants to be an Intelligence Community contractor, it can't also be a data broker selling the location data of intelligence officers. That provision would address a real counterintelligence vulnerability and I am dismayed that my amendment to include it in this year's bill was rejected by a party-line vote.

I also filed two amendments to the classified annex to address intelligence activities about which I have deep concerns. I submitted these amendments five days prior to the committee mark-up of this bill, but regrettably the Chairman and the Majority refused to vote on these amendments and denied me the opportunity to even discuss the underlying, troubling intelligence activities. I have served on this Committee for more than twenty-five years and do not recall a single instance in which the Committee rejected an amendment to the classified annex from any consideration at all, regardless of when it was submitted. It is a sad irony that, almost fifty years to the day after the Senate created the Select Committee on Intelligence, the Chairman and Majority set out to prevent debate on the annual authorization of classified activities, one of the Committee's most important oversight responsibilities.

RON WYDEN.

MINORITY VIEWS OF SENATOR MARTIN HEINRICH AND SENATOR RON WYDEN

We voted against the Intelligence Authorization Act because of deep concerns about the markup process, which denied necessary debate on certain classified activities. We are also concerned about the activities themselves and their support in the classified annex.

MARTIN HEINRICH.
RON WYDEN.

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.

○