Calendar No. 504

114TH CONGRESS *2d Session* | SENATE | REPORT 114–277

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017

JUNE 15, 2016.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 3017]

The Select Committee on Intelligence, having considered an original bill (S. 3017) to authorize appropriations for fiscal year 2017 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

CLASSIFIED ANNEX TO THE COMMITTEE REPORT

On February 9, 2016, acting 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 that the President's aggregate request for the National Intelligence Program for Fiscal Year 2017 is $53.5 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 (the "Act") and has the legal sta-

tus 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 2017 that is being reported by the Committee.

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2017.

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 2017 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 in the amount of $568,596,000 for the Intelligence Community Management Account (ICMA) of the Office of the Director of National Intelligence for the elements within the ICMA for Fiscal Year 2017.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for Fiscal Year 2017 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 301. Restriction on conduct of intelligence activities

Section 301 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

Section 302. Increase in employee compensation and benefits authorized by law

Section 302 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.

Section 303. Support to nonprofit organizations assisting intelligence community employees

Section 303 permits the Director of National Intelligence (DNI) to engage in fundraising in an official capacity for the benefit of nonprofit organizations that provide support to surviving family members of a deceased employee of an element of the Intelligence Community or otherwise provide support for the welfare, education, or recreation of Intelligence Community employees, former employees, or their family members. Section 303 further requires that the DNI and the Director of the Central Intelligence Agency notify the congressional intelligence committees at least thirty days before they engage in such fundraising (or at the time they decide to participate, whichever is earlier).

Section 304. Promotion of science, technology, engineering, and math education in the intelligence community

Section 304 requires the Director of National Intelligence to submit a five-year investment strategy for outreach and recruiting efforts in the fields of science, technology, engineering, and mathematics (STEM), to include cybersecurity and computer literacy. Section 304 further requires elements of the Intelligence Community to submit STEM investment plans supporting this strategy for each of the fiscal years 2018 through 2022, along with the materials justifying the budget request of each element for these STEM recruiting and outreach activities.

Section 305. Retention of employees of the intelligence community who have science, technology, engineering, or math expertise

Section 305 authorizes a new payscale to permit salary increases for employees in the Intelligence Community with STEM backgrounds. Section 305 also requires notifications to individual employees if a position is removed from this new payscale. Section 305 further requires the head of each Intelligence Community element to submit to the congressional intelligence committees a report on the new rates of pay and number of positions authorized under this payscale.

Section 306. Annual review and report on interactions between the intelligence community and entertainment industry

Section 306 requires the Director of National Intelligence to provide an annual report to the congressional intelligence committees detailing interactions between the Intelligence Community and the entertainment industry. Section 306 also requires the report to include a description of the nature, duration, costs, and results of each engagement, as well as a certification that each engagement did not result in a disclosure of classified information and whether any information was declassified for the disclosure. Section 306 further requires that before an Intelligence Community element may engage with the entertainment industry, the head of that element must approve the proposed engagement and notify the congressional intelligence committees at least thirty days in advance of why the engagement would further the Intelligence Community element's interests.

These engagements, some of which have been described in partially declassified inspector general reports, cost taxpayer dollars,

raise potential ethics concerns, increase the risk of disclosure of classified information, and consume the time and attention of Intelligence Community personnel responsible for United States national security. Neither the production of entertainment nor the self-promotion of Intelligence Community entities are legitimate purposes for these engagements.

Section 307. Protections for independent inspectors general of elements of the intelligence community

Section 307 requires the Inspector General for each Intelligence Community element to implement a policy that prohibits Office of Inspector General senior employees from being involved in matters that affect the interest of an organization within an element for which the employee worked for at least two years, and that prohibits Office of Inspector General non-senior employees from being involved in matters that affect the interest of an organization within an agency for which the employee worked for at least one year. Section 307 further prohibits the Director of National Intelligence from requiring an employee of an Office of Inspector General to rotate to a position in the element for which such office conducts oversight.

Section 308. Congressional oversight of policy directives and guidance

Section 308 requires the Director of National Intelligence to submit to the congressional intelligence committees notifications and copies of any classified or unclassified Presidential Policy Directive, Presidential Policy Guidance, or other similar policy document issued by the President which involves the Intelligence Community, within the specified timeframes. Section 308 further requires the Director to notify the congressional intelligence committees of guidance to implement such policies.

Section 309. Notification of memorandums of understanding

Section 309 requires the head of each element of the Intelligence Community to submit to the congressional intelligence committees copies of each memorandum of understanding or other agreement regarding intelligence activities entered into with another entity of the federal government within specified timeframes.

Section 310. Intelligence community assistance for nationally significant critical infrastructure

Section 310 requires the Director of National Intelligence and the Secretary of Homeland Security to establish a program to provide assistance and support to certain critical infrastructure entities, on a voluntary basis, for the purpose of reducing the likelihood of catastrophic harm resulting from a cyber attack.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 401. Designation of the Director of the National Counterintelligence and Security Center

Section 401 renames the National Counterintelligence Executive as the "National Counterintelligence and Security Center," with conforming amendments.

SUBTITLE B—OTHER ELEMENTS

Section 411. Enhanced death benefits for employees of the Central Intelligence Agency

Section 411 authorizes the Director of the Central Intelligence Agency to pay death benefits substantially similar to those authorized for members of the Foreign Service, and requires the Director to submit implementing regulations to the congressional intelligence committees.

Section 412. Pay and retirement authorities of the Inspector General of the Central Intelligence Agency

Section 412 amends the Central Intelligence Agency Act of 1949 to authorize the Inspector General (IG) of the Central Intelligence Agency (CIA) to consider certain positions as law enforcement officers for purposes of calculating retirement eligibility and entitlements under chapters 83 and 84 of title 5, United States Code, if such officer or employee is appointed to a position with responsibility for investigating suspected offenses against the criminal laws of the United States. Section 412 may not be construed to confer on the IG of the CIA, or any other officer or employee of the CIA, any police or law enforcement or internal security functions or authorities.

Section 413. Prohibition on the Director of the National Security Agency serving contemporaneously as a commander of a combatant command

Section 413 amends the National Security Act of 1959, 50 U.S.C. § 3602(a), to prohibit the Director of the National Security Agency from concurrently serving as the commander of a unified combatant command within the Department of Defense, as defined in 10 U.S.C. § 161(c).

Section 414. Enhancing the technical workforce for the Federal Bureau of Investigation

Section 414 requires the Federal Bureau of Investigation (FBI) to produce a comprehensive strategic workforce report to demonstrate progress in expanding initiatives to effectively integrate information technology expertise in the investigative process. Section 414 further requires the report to include: (1) progress on training, recruitment, and retention of cyber-related personnel; (2) an assessment of whether FBI officers with these skill sets are fully integrated in the FBI's workforce; (3) the FBI's collaboration with the private sector on cyber issues; and (4) an assessment of the utility of reinstituting and leveraging the FBI Director's Advisory Board.

TITLE V—MATTERS RELATING TO FOREIGN COUNTRIES

Section 501. Committee to counter active measures by the Russian Federation to exert covert influence over peoples and governments.

Section 501 requires the President to establish an interagency committee to counter active measures by the Russian Federation that constitute Russian actions to exert covert influence over peoples and governments.

Section 502. Limitation on travel of accredited diplomats of the Russian Federation in the United States from their diplomatic post

Section 502 requires the Director of the Federal Bureau of Investigation to certify that Russian diplomats have followed proper travel notification procedures before the Secretary of State can permit Russian diplomats' travel in excess of 50 miles outside of their diplomatic posts.

Section 503. Study and report on enhanced intelligence and information sharing with Open Skies Treaty member states

Section 503 requires the Director of National Intelligence to conduct a study to determine the feasibility of creating an intelligence sharing arrangement and database among parties to the Open Skies Treaty with higher frequency, quality, and efficiency. Section 503 also requires the Director to issue a report as to how the Russian Federation is using Open Skies Treaty collection, a list of the covered parties that have been updated with this information, and an analysis of the benefits the United States derives by being a party to the treaty as well as the potential implications for covered state parties if the United States should withdraw from the treaty.

Section 504. Reviews on cooperation between the intelligence community and foreign intelligence entities

Section 504 requires the Director of National Intelligence to review the number, scope, purpose, benefits, and risks of the relationships between the Intelligence Community and foreign intelligence entities and to report to the congressional intelligence committees on specified findings. Section 504 further requires the Director of the Central Intelligence Agency to review its coordination of the relationships between the elements of the Intelligence Community and foreign intelligence entities and report to the congressional intelligence committees on specified findings.

TITLE VI—PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Section 601. Information on activities of the Privacy and Civil Liberties Oversight Board

Section 601 requires the Privacy and Civil Liberties Oversight Board to keep Congress and relevant Intelligence Community elements fully and currently informed of its activities.

Section 602. Appointment of staff of the Privacy and Civil Liberties Oversight Board

Section 602 amends the Intelligence Reform and Terrorism Prevention Act of 2004, 42 U.S.C. § 2000ee(j), to require that, in the

absence of a chairman, the members of the Privacy and Civil Liberties Oversight Board (the "Board") may, by unanimous vote, exercise the chairman's authority to appoint and fix the compensation of Board personnel. The Committee appreciates the professionalism of the Board's staff. However, the Committee is concerned that the staff of the Board may lack an appropriate balance in expertise and that this imbalance may impede the efforts of the Board to execute its statutory mandate to consider the appropriate balance between counterterrorism efforts of the United States and the privacy and civil liberties as guaranteed by the United States Constitution. Therefore, the Committee strongly recommends that the Board make every effort to recruit, hire or appoint, and retain staff, employees, detailees, experts, and consultants who have relevant expertise and experience in both efforts to protect the United States from terrorism and with privacy and civil liberties as guaranteed by the United States Constitution.

Section 603. Protection of the privacy and civil liberties of United States persons

Section 603 ensures that the Privacy and Civil Liberties Oversight Board (the "Board") is focused on the privacy and civil liberties of United States persons when conducting its analysis and review of United States counterterrorism efforts.

The Committee notes that the August 2004 Executive Order 13353 provided the foundation for the Board by creating an entity within the Department of Justice that would "protect the legal rights of all Americans, including freedoms, civil liberties, and information privacy guaranteed by Federal law, as the President may direct."

Similarly, the Committee recognizes that the Intelligence Reform and Terrorism and Prevention Act of 2004 (IRTPA), 42 U.S.C. § 2000ee(c)(1) and (2) states that the Board "shall (1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."

That same language is repeated in the report to accompany IRTPA, H. Rept. 108–796, 108th Cong. 2d Sess. (Dec. 7, 2004) (the Board "is charged with ensuring that privacy and civil liberties concerns are appropriately considered in the implementation of laws, regulations, and policies of the government related to efforts to protect the Nation against terrorism").

Notably, Senator Collins, the original sponsor of IRTPA, emphasized this intent on the Senate Floor, stating that the transparency resulting from the Board's activities "helps to give confidence to the American people that the protection of their civil liberties and privacy is being addressed as we take actions to further protect our Nation from terrorism." Cong. Rec. S11974 (daily ed. Dec. 8, 2004) (statement of Senator Collins).

The Committee believes it is important for the Board to consider the privacy and civil liberties of U.S. Persons first and foremost when conducting its analysis and review of United States counterterrorism efforts.

TITLE VII—MATTERS RELATING TO UNITED STATES NAVAL STATION, GUANTANAMO BAY, CUBA

Section 701. Declassification review of information on Guantanamo detainees and mitigation measures taken to monitor the individuals and prevent future attacks

Section 701 requires the Director of National Intelligence to complete a declassification review of information on the past terrorist activities of detainees transferred or released from Guantanamo, make resulting declassified information publicly available, and submit to the congressional intelligence committees a report setting forth the results of the declassification review and, if any information covered by the review was not declassified, a justification for the determination not to declassify such information. Section 701 also sets the schedule for such reviews and requires that the reviews and reports include mitigation measures being taken by the country where the individual has been transferred or released to monitor and prevent the individual from carrying out future terrorist activities. Section 701 further defines past terrorist activities to include terrorist organization affiliations, terrorist training, role in terrorist attacks, responsibility for the death of United States citizens or members of the Armed Forces, any admission thereof, and a description of the intelligence supporting the past terrorist activities, including corroboration, confidence level, and any dissent or reassessment by the Intelligence Community.

Section 702. Limitation on transfer of Guantanamo detainees to foreign countries

Section 702 prohibits an individual detained at Guantanamo from being transferred or released to a foreign country until after the date that the Director of National Intelligence certifies that an intelligence driven threat monitoring system has been established and is sufficient to mitigate the risk of such individuals reengaging in terrorism or posing a threat to United States persons or national security, and that the Intelligence Community has the capability to monitor all such individuals by appropriate means to provide assessments on their activities as required.

TITLE VIII—REPORTS AND OTHER MATTERS

Section 801. Submission of intelligence related information in certain reports by the Secretary of Defense

Section 801 prohibits the Secretary of Defense from using waiver authority under 10 U.S.C. § 119(e)(1) to omit reporting intelligence or intelligence-related activities in the annual report requirements.

Section 802. Cyber Center for Education and Innovation Home of the National Cryptologic Museum

Section 802 amends 10 U.S.C. § 449 to enable the establishment of a Cyber Center for Education and Innovation Home of the National Cryptologic Museum.

Section 803. Counterintelligence access to telephone toll and transactional records.

Section 803 makes a conforming edit to 18 U.S.C. § 2709, to clarify that the government is permitted to obtain non-content elec-

tronic communications transactional records (commonly known as "ECTRs") from wire or electronic communication service providers in national security investigations upon proper certification of the Director of the Federal Bureau of Investigation (FBI) or the Director's designee.

In 1986, Congress enacted Section 2709 to allow the FBI to request telephone subscriber information, toll billing records, and electronic communications transactional records in national security investigations and imposed a duty on wire and electronic communication service providers to comply with such requests. This duty has remained unchanged since Section 2709's enactment.

Unfortunately, when Congress amended the required certification language in Section 2709(b) in 1993, it inadvertently omitted electronic communications transactional records among the list of records that required a certification from the FBI. Since Section 2709(a) still imposed a duty on providers to comply with requests for electronic communications transactional records, the FBI continued to issue requests for these transactional records and the providers continued to comply.

Beginning in 2009, certain major electronic communications service providers began refusing to comply with FBI requests for electronic communications transactional records under Section 2709. The service providers justified their non-compliance on the absence of a specific mention of "electronic communications transactional records" in the required certification provision of Section 2709(b). The non-compliance of certain companies made it much more difficult for the FBI to obtain these electronic communications transactional records. Instead of being able to rely upon a properly-certified request for electronic communications transactional records under Section 2709—which could be issued by the FBI in a matter of days—the FBI has been required to seek the very same electronic communications transactional records from non-compliant providers through the use of a business records court order under the Foreign Intelligence Surveillance Act, a process that often takes over a month. Notably, a 2014 Department of Justice Inspector General Report states that, after certain providers began to refuse to comply with FBI requests for electronic communications transactional records, a request under Section 2709 that had taken "a matter of hours if necessary, now takes about 30–40 days to accomplish[.]" United States Dep't of Justice, Office of Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009*, at 73 (August 2014).

In 2010, the Department of Justice began seeking a legislative clarification of Section 2709 to address the problem caused by the non-compliant providers. Director Comey testified at a Senate Judiciary Committee hearing in December 2015 that a change to the electronic communications transactional records provision

> would be enormously helpful. . . . It would save us a tremendous amount of work hours if we could fix that, without any compromise to anyone's civil liberties or civil rights. Everybody who has stared at this has said, "that's actually a mistake. We should fix that."

Additionally, in response to a question posed at this Committee's 2016 Worldwide Threats hearing, Director Comey stated that the FBI needs

> [a clarification to the electronic communications transactional records provision] very much and it's actually quite an ordinary fix that is necessary because what I believe is a typo in the 1993 statute that has led to some companies interpreting it in a way I don't believe Congress ever intended. And so it is ordinary, but it affects our work in a very, very big and practical way.

Director Comey also confirmed that it was a "top legislative priority" for the FBI. Thus, certain providers' noncompliance is substantially impairing the FBI's ability to conduct national security investigations. Because of this resulting operational impairment, the Administration initially requested the legislative clarification in 2010 for the Fiscal Year 2011 authorization bill. Similarly, on May 24, 2016, the Department of Justice reiterated in a formal written proposal to the Committee the Administration's request for the legislative clarification to Section 2709. The current Administration has now twice requested that Congress clarify the technical error in Section 2709. Ultimately, the Committee approved an amendment to Section 2709(b), which also clarifies that "electronic communications transactional records" do not contain content.

Section 804. Oversight of national security systems

Section 804 amends 44 U.S.C. § 3557 to codify and strengthen existing roles and responsibilities with regard to the oversight of national security systems.

Section 805. Joint facilities certification

Section 805 requires that before an element of the Intelligence Community purchases, leases, or constructs a new facility that is 20,000 square feet or larger, the head of that element must first certify that all prospective joint facilities have been considered, that it is unable to identify a joint facility that meets its operational requirements, and it must list the reasons for not participating in joint facilities in that instance.

Section 806. Improvement of leadership and management of space activities

Section 806 requires the Director of National Intelligence (DNI), in collaboration with the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, to issue an update to the strategy for a comprehensive review of the United States national security overhead satellite architecture required in the Intelligence Authorization Act for Fiscal Year 2016. Section 806 requires the DNI, in coordination with the Secretary of Defense, to submit a plan to harmonize the Intelligence Community's governance, operations, analysis, and collection activities related to space and counterspace under the oversight of a single official, to be appointed by the DNI, in consultation with the Secretary of Defense. Section 806 also requires the DNI to submit a workforce plan for space and counterspace operations, policy, acquisition, and analysis. Section 806 further requires the Director of the National Reconnaissance

Office and the Commander of U.S. Strategic Command to submit a concept of operations and requirements documents for the Joint Interagency Combined Space Operations Center.

Section 807. Advances in life sciences and biotechnology

The Committee recognizes the rapid advancements in the life sciences and biotechnology and firmly believes that biology in the twenty-first century will transform the world as physics did in the twentieth century.

The potential risks associated with these advancements are less clear. The posture of the Intelligence Community to follow and predict this rapidly changing landscape is a matter of concern recognizing the global diffusion and dual-use nature of life sciences and biotechnology along with the dispersed responsibility of the life sciences related issues across several National Intelligence Officer portfolios.

Section 807 requires the Director of National Intelligence to brief the congressional intelligence committees on a proposed plan and actions to monitor advances in life sciences and biotechnology to be carried out by the Director. The Director's plan should include, first, a description of the Intelligence Community's approach to leverage the organic life science and biotechnology expertise both within and outside the Intelligence Community; second, an assessment of the current life sciences and biotechnology portfolio, the risks of genetic editing technologies, and the implications of these advances on future biodefense requirements; and, third, an analysis of organizational requirements and responsibilities to include potentially creating new positions. Section 807 further requires the Director to submit a written report and provide a briefing to the congressional intelligence committees on the role of the Intelligence Community in the event of a biological attack, including a technical capabilities assessment to address potential unknown pathogens.

Section 808. Reports on declassification proposals

Section 808 requires the Director of National Intelligence to provide the congressional intelligence committees with a report and briefing on the Intelligence Community's progress in producing four feasibility studies undertaken in the course of the Intelligence Community's fundamental classification guidance review, as required under Executive Order 13526. Section 808 further requires the Director to provide the congressional intelligence committees with a briefing, interim report, and final report on the final feasibility studies produced by elements of the Intelligence Community and an implementation plan for each initiative.

Section 809. Improvement in government classification and declassification

Section 809 requires Executive Branch agencies and departments to review their classification guidance documents every five years. Section 809 further requires the Director of National Intelligence to provide an annual written notification to the congressional intelligence committees certifying the creation, validation, or substantial modification (to include termination) of existing and proposed controlled access programs, and the compartments and subcompartments within each.

Section 810. Report on implementation of research and development recommendations

Section 810 requires the Director of National Intelligence to conduct and provide to the congressional intelligence committees a current assessment of the Intelligence Community's implementation of the recommendations issued in 2013 by the National Commission for the Review of the Research and Development (R&D) Programs of the Intelligence Community.

Section 811. Report on Intelligence Community Research and Development Corps

Section 811 requires the Director of National Intelligence to develop and brief the congressional intelligence committees on a plan, with milestones and benchmarks, to implement a R&D Reserve Corps, as recommended in 2013 by the bipartisan National Commission for the Review of the R&D Programs of the Intelligence Community, including any funding and potential changes to existing authorities that may be needed to allow for the Corps' implementation.

Section 812. Report on information relating to academic programs, scholarships, fellowships, and internships sponsored, administered, or used by the intelligence community

Section 812 requires the Director of National Intelligence to submit to congressional intelligence committees a report on information that the Intelligence Community collects on certain academic programs, scholarships, and internships sponsored, administered, or used by the Intelligence Community.

COMMITTEE COMMENTS

Commercial Geospatial Intelligence Strategy

The Committee applauds the National Geospatial-Intelligence Agency (NGA) for issuing its October 2015 Commercial Geospatial Intelligence (GEOINT) Strategy, which states a goal of fostering a "more diverse, resilient, agile, and responsive GEOINT program that provides seamless user access to the best mix of commercial GEOINT . . . to fulfill National System for Geospatial-Intelligence (NSG) and Allied System for Geospatial-Intelligence (ASG) mission needs." The Committee also finds merit in the NGA's "GEOINT Pathfinder" project, which seeks to maximize the use of unclassified and commercially available data sources that can be easily and rapidly shared with a variety of military, United States and allied government, and non-government customers, and supports the project's continuation and expansion.

The Committee commends the NGA for pursuing new methods of intelligence collection and analysis to inform, complement, and add to its support of warfighter requirements by looking to emerging commercial technology providers, including small satellite companies, which hold the promise of rapid technological innovation and potentially significant future cost savings to the U.S. taxpayer. The Committee further encourages the Director of the NGA to ensure sufficient funding is available to acquire new, unclassified sources, including commercial satellite imagery providing unprecedented global persistence, as well as products and services that provide in-

formation and context about change relevant to geospatial intelligence. The Committee also encourages the NGA to pursue new business models, including commercial acquisition practices, to enable the NGA's access to data, products, and services in ways consistent with best commercial practices.

The Committee fully supports the NGA's course of action in partnering with the commercial GEOINT industry to meet future warfighter intelligence requirements, while recognizing the need to take appropriate steps to protect national security, and encourages the Director of the NGA and the Under Secretary of Defense for Intelligence to keep the Committee informed of their progress in implementing this strategy. In building future year budgets, the Committee strongly encourages the Department to ensure continued funding is provided for implementation through at least Fiscal Year 2021.

Space launch facilities

The Committee continues to believe it is critical to preserve a variety of launch range capabilities to support national security space missions. Spaceports or launch and range complexes may provide capabilities to reach mid-to-low or polar-to-high inclination orbits. The Committee believes an important component of this effort may be state-owned and operated spaceports that are commercially licensed by the Federal Aviation Administration, which leverage non-federal public and private investments to bolster U.S. launch capabilities. Additionally, the Committee believes that these facilities may be able to provide additional flexibility and resilience to the Nation's launch infrastructure, especially as the nation considers concepts such as the reconstitution of satellites to address the growing foreign counterspace threat. The Committee notes recent testimony by the Chief of Staff of the U.S. Air Force, General Mark Welsh, who stated,

> As we look at this space enterprise and how we do it differently in the future, as we look more at disaggregation, microsats, cube sats, small sats, things that don't have to go from a large launch complex all the time, I think proliferating launch complexes is probably going to be a natural outshoot of this. I think it's commercially viable, it may be a way for companies to get into the launch business who could not afford to get into it or don't see a future in it and for large national security space launches, but I think this has got to be part of the strategy that this whole national team puts together as we look to the future.

Therefore, the Committee encourages the Intelligence Community, in partnership with the U.S. Air Force, to consider the role and contribution of spaceports or launch and range complexes to our national security space launch capacity, and directs the Office of the Director of National Intelligence, in consultation with the Department of Defense and the U.S. Air Force, to brief the Committee on their plans to utilize such facilities.

National reconnaissance office workforce optimization strategy

The Committee has had longstanding interest in, and support for, a permanent government cadre to provide the National Reconnaissance Office (NRO) with a stable, expert acquisition workforce. The Committee applauds the substantial progress that the NRO has made in the past year in this regard. The Committee has parallel interests in providing the IC with flexibility to manage a multi-sector workforce and in continuing the reduction in the reliance on contractors.

Therefore, the Committee directs the NRO to conduct a workforce review to optimize the mix between government civilians and contractors and report to the Committee with a strategy within 90 days of enactment of this Act.

Office of the Inspector General, Central Intelligence Agency

The previous Inspector General of the CIA departed from the position on January 31, 2015. The President has not yet nominated a candidate for the Senate's consideration. The Committee believes it is critical that the Office of the Inspector General (OIG) be headed by a Senate-confirmed officer fully able to exercise the authorities and independence provided the position in statute.

COMMITTEE ACTION

On May 24, 2016, a quorum being present, the Committee met to consider the bill and amendments. The Committee took the following actions:

Votes on amendments to committee bill, this report and the classified annex

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

By voice vote, the Committee adopted en bloc seven amendments to the classified annex sponsored by: (1) Chairman Burr and Vice Chairman Feinstein; (2) Senator Rubio; (3) Senator Rubio and Senator Lankford; (4) Senator Warner; (5) Senator Warner and Senator Blunt; (6) Senator King, Senator Lankford, and Senator Rubio; and (7) Senator Cotton and Senator Rubio.

By voice vote, the Committee adopted *en bloc* the following seven amendments to the bill: (1) an amendment by Chairman Burr and Vice Chairman Feinstein to enhance the Federal Bureau of Investigation's workforce; (2) an amendment by Chairman Burr, Vice Chairman Feinstein, Senator Warner, and Senator Cotton that permits the Director of National Intelligence to support nonprofit organizations assisting Intelligence Community employees and their families; (3) an amendment by Vice Chairman Feinstein to require notifications of engagements of the Intelligence Community with the entertainment industry; (4) an amendment by Vice Chairman Feinstein and Senator Hirono to improve government classification and declassification; (5) an amendment by Senator Rubio to limit the transfers of detainees to certain countries; (6) an amendment by Senator Warner, Senator Mikulski, and Senator Hirono to require reporting on Intelligence Community academic programs; and (7) an amendment by Senator Collins, Senator Coats, Senator Mi-

kulski, Senator Heinrich, Senator Hirono, Senator Risch, and Senator Warner to require Intelligence Community assistance for nationally significant critical infrastructure.

By a vote of 3 ayes to 12 noes, the Committee rejected an amendment by Senator Wyden, Senator Heinrich, and Senator Hirono to strike Section 603 of the bill. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Vice Chairman Feinstein—no; Senator Wyden—aye; Senator Mikulski—no; Senator Warner—no; Senator Heinrich—aye; Senator King—no; Senator Hirono—aye.

By voice vote, the Committee adopted an amendment by Senator Rubio to the classified annex, as modified by a second degree amendment by Vice Chairman Feinstein.

By a vote of 12 ayes to 3 noes, the Committee adopted an amendment by Senator Collins to provide the Inspector General of the Central Intelligence Agency with certain pay and retirement authorities. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Lankford—no; Senator Cotton—aye; Vice Chairman Feinstein—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Senator Hirono—aye.

By a vote of 12 ayes to 3 noes, the Committee adopted an amendment by Senator Cotton, as modified by a second degree amendment by Vice Chairman Feinstein, to clarify that the Government may obtain electronic communication transactional records from information service providers, as well as telecommunications providers. The votes in person or by proxy were as follows: Chairman Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Lankford—aye; Senator Cotton—aye; Vice Chairman Feinstein—aye; Senator Wyden—no; Senator Mikulski—aye; Senator Warner—aye; Senator Heinrich—no; Senator King—aye; Senator Hirono—no.

By voice vote, the Committee adopted an amendment by Senator Cotton, as modified by three separate second degree amendments by Chairman Burr, Vice Chairman Feinstein, and Senator King, to require the Director of National Intelligence to lead a process for declassifying and making publicly available information on released Guantanamo detainees.

Vote to report the committee bill

The Committee voted to report the bill, as amended, by a vote of 14 ayes and 1 no. The votes in person or by proxy were as follows: Chairman Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Lankford—aye; Senator Cotton—aye; Vice Chairman Feinstein—aye; Senator Wyden—no; Senator Mikulski—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; and Senator Hirono—aye.

By unanimous consent, the Committee authorized the staff to make technical and conforming changes in the bill, report, and classified annex, following the completion of the mark-up.

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 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 June 3, 2016, 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 SENATOR WARNER

I am happy that the range of amendments I offered this year have all been accepted into the bill, including a number of provisions relating to my priorities of modernizing how the nation undertakes its planning for, and acquisition of, overhead satellite systems, including better coordination and collaboration between the Intelligence Community (IC) and the Department of Defense.

I commend the Committee for diligently listening to the calls that I and other Committee colleagues, including Senators King, Mikulski, Hirono, Rubio and others, have made to closely monitor this critical area of our national intelligence program.

The bill directs the Director of National Intelligence, the Secretary of Defense and Chairman of the Joint Chiefs to update and deliver to the Committee the strategy we called for in last year's bill for a comprehensive approach to the overhead satellite architecture that supports U.S. intelligence programs.

Such a strategy must ensure that the nation's satellite architecture meets the nation's needs in peace- and war-time; responsibly stewards the taxpayers' dollars; accurately takes into account cost- and performance tradeoffs of the architecture; meets realistic requirements; produces and fosters excellence, innovation and competition; produces innovative satellite systems in under five years that can leverage common, standardized design elements and commercially-available technologies; takes advantage of rapid advances in commercial technology, innovation and commercial-like acquisition practices; and fosters competition and a robust industrial base.

My focus this year has also been to encourage the IC to take advantage of the large number of overhead commercial and emerging small satellite technologies that we expect to see launched as soon as this year. The Community needs to be prepared to take advantage of these resources and not to see them as competition. Consistent with the National Space Policy, the U.S. government should make maximum use of commercial space capabilities and acquisition practices for national security systems where the required performance can be met with commodity technology to reduce acquisition timelines and costs, promote competition, capitalize on the pace of commercial technology advances, and avoid unnecessary government-unique investments.

I, along with my Committee colleagues, have commended the Community, and especially the National Geospatial-Intelligence Agency (NGA) for pursuing new methods of intelligence collection and analysis to inform, complement, and add to its support of warfighter requirements by looking to emerging commercial technology providers, including small satellite companies, which hold the promise of rapid technological innovation and potentially significant future cost savings to the U.S. taxpayer.

As the Director of NGA, Robert Cardillo, noted last year, "we are in the middle of an explosion of innovation across the geospatial community. . . . I call this explosion the 'democratization' of geospatial information. This 'democratization' makes geospatial intelligence increasingly transparent because of the huge number and diversity of commercial and open sources of information." He went on to say, "the combined possibilities of an emergent commercial space market, the small satellite revolution, and a vibrant community of companies already mining the possibilities of geospatial data has inspired us to seek new opportunities.Let me reiterate—NGA wants to be the partner of choice for advancing our craft and enabling consequence by cooperating, not competing with, industry."

At the same time, my intent is not to undercut, or reduce current arrangements the Community has for acquiring commercial overhead imagery, which have worked exceptionally well—including through the "Enhanced View" arrangement. I would like to see the Community "expand the pie" of available commercial data, not to shrink what has been working well, as we prepare for new technologies to come on line.

Elsewhere in the bill, I was happy to see the emphasis on the need to enhance the way the Community undertakes research and development (R&D). Building upon the work of the 2013 National Commission for the Review of the R&D Programs of the IC, provisions I offered require the DNI to develop a plan to implement an "R&D Reserve Corps," as recommended by the Commission, and to provide an updated assessment of the Community's implementation of Commission's recommendations.

A provision I offered with Senator Mikulski calls on the IC to provide metrics of how well they are doing at hiring talented individuals who have gone through IC-supported academic programs such as the NSA and DHS National Centers of Academic Excellence in Information Assurance and Cyber Defense Education (such as those at Virginia academic institutions including at George Mason University, Hampton University, James Madison University, Lord Fairfax Community College, Marymount University, Norfolk State University, Northern Virginia Community College, Radford University, Tidewater Community College, and Virginia Tech).

Another provision I offered with Senator Blunt authorizes funds to operate a Childcare Center at the National Geospatial-Intelligence Agency's headquarters at Fort Belvoir, which is much needed by the intelligence professionals who work there to keep the nation safe, and where the childcare center building has not been operational since it was built two years ago.

A provision I offered calls upon the IC, in partnership with the U.S. Air Force, to consider the role and contribution to our national security space launch capacity of spaceports or launch and range complexes that are state-owned and operated, and commercially licensed by the Federal Aviation Administration—such as Virginia's Wallops Island. In supporting this provision the Committee cites the Chief of Staff of the U.S. Air Force, General Mark Welsh, who recently stated, "As we look at this space enterprise and how we do it differently in the future, as we look more at disaggregation,

microsats, cube sats, small sats, things that don't have to go from a large launch complex all the time, I think proliferating launch complexes is probably going to be a natural outshoot of this. I think it's commercially viable, it may be a way for companies to get into the launch business who could not afford to get into it or don't see a future in it and for large national security space launches, but I think this has got to be part of the strategy that this whole national team puts together as we look to the future."

In closing, I wish to reiterate how proud I am to represent the thousands of current and former members of the intelligence agencies who live, work, or retire in Virginia. Because they are not able to discuss their very important work with friends and even family members, I will continue to be a strong advocate for them in Congress, and will continue to pursue efforts to recognize and honor their contributions to the nation.

MARK R. WARNER

ADDITIONAL VIEWS OF SENATOR COATS

The Defense Intelligence Agency (DIA) is unique among its peer agencies in the Intelligence Community, as it's charged with twin obligations that complement and at times conflict with one another. The DIA's role as the premier combat support agency and a national intelligence organization demand steady leadership and an unshakable commitment to analytic objectivity in the face of departmental allegiance or a sense of owed deference to the military rank structure. In my view, the DIA's continued stewardship by a uniformed military officer is irreconcilable with this aspiration.

As overseer for the entirety of the Defense Intelligence Enterprise (DIE), the Director of the DIA is charged with responsibilities that extend far beyond the agency itself. The DIE is a community within a community, comprising the DIA, Service Intelligence Centers, and the respective intelligence centers of the various Combatant Commands. The tension underlying this arrangement is a function of protocol and military deference. While the DIA is a three-star command within the Department of Defense (DOD) construct, the intelligence operations in many of the DIE's constituent entities function under the aegis of four-star commands—and specifically, the four-star general leading those commands.

The sum of these underlying structural realities is that a three-star general is ostensibly responsible for the analytic quality and objectivity of DIA analysts who—as a function of proximity and organizational architecture—work under four-star generals. The problem with this construct should be self-evident. If not, a demonstrative example can be found in allegations that intelligence analysis was deliberately manipulated at U.S. Central Command's Joint Intelligence Center (JICCENT) to favor desired policy outcomes. Notably absent from this episode is the DIA Director's exercise of evocative supervisory responsibility over the JICCENT work product, which would be in fact anathema to the command and rank structure within which the DIA and U.S. Central Command exist in relation to one another.

While my concerns are most acutely agitated by the referenced allegations, they do not end there. The DIA faces systemic issues, including incoherence of mission, resistance to change, and unwillingness to meaningfully define its customer base. The agency faces seemingly limitless intelligence requirements and unique structural challenges that hinder its ability to satisfy customers in the DOD, Military Departments, Unified Combatant Commands, and the broader Intelligence Community (IC). The present approach appears instead to be a mechanical assumption of responsibility for any conceivable intelligence requirement that a boundless population of customers might level on the DIA. Surely, this is inconsistent with the cultivation of deep-seated professional expertise,

proficiency, and organizational identity. At a minimum, it is inefficient and unsustainable.

In the course of our Committee debate on the Intelligence Authorization Act for Fiscal Year 2017, I introduced an amendment that would mandate a transition to civilian leadership at the DIA. I do not take lightly the intent, and I am sensitive to the deviation from historical precedent. I am nonetheless compelled to advocate for this change in the DIA's leadership construct. It is a necessary step toward addressing an agency beset by the challenges I have outlined, although I recognize it will not on its own resolve all of them. Civilian leadership of the DIA would in my view change the obstructive dynamic that presently defines the agency's relationship with important DIE constituents, not the least of which are the Combatant Commands—and especially U.S. Central Command. With operational responsibility for wars in Syria, Iraq, and Afghanistan, the intelligence produced under U.S. Central Command auspices must be incorruptible in practice and perception. Present circumstances, however, invite the opposite judgment.

While the ultimate version of the bill that was reported to the full Senate did not include my proposed amendment, I am hopeful this discussion will continue within the Committee, between the Armed Services and Intelligence Committees, and with the IC and DOD. The intelligence needs of the U.S. warfighter, and the broader national security ecosystem, demand that we cooperatively address this issue.

DAN COATS.

ADDITIONAL VIEWS OF SENATORS HEINRICH AND HIRONO

This important bill authorizes funding for key intelligence priorities, including programs to address the threat of terrorism. We supported the bill during Committee consideration, and look forward to further discussion as the bill moves forward, especially on those provisions that have not yet been subject to public debate.

We are particularly concerned about two provisions in the bill.

The first is a provision added to the bill by amendment. This amendment would grant new authority to the FBI to obtain electronic communication transactional records (ECTRs) using National Security Letters (NSLs), which compel recipients to allow government access to records without a court order.

The FBI has compared expanding these authorities to fixing a "typo" in the Electronic Communications Privacy Act (ECPA). However, during consideration of ECPA reform legislation in 1993, the House Judiciary Committee said in its committee report that "Exempt from the judicial scrutiny normally required for compulsory process, the national security letter is an extraordinary device. New applications are disfavored."

The House Judiciary Committee report also makes clear that the bill's changes to Section 2709(b) of ECPA were a "modification of the language originally proposed by the FBI."

This does not support claims that the removal of the ECTR language was a "typo."

Instead, the ECTR amendment to this bill represents a vast expansion of FBI authorities. Currently, the FBI is permitted to use NSLs only to obtain basic subscriber information about telecommunications—name, address, length of service, and local and long distance toll billing records. However, this amendment would broaden that list to include electronic communication transactional records, which the FBI could then obtain from service providers by merely certifying relevance to an investigation with no court order required.

The FBI can already obtain ECTRs with a court order using other authorities, but this broad new authority would allow the FBI to obtain internet transactional information that is far more revealing than phone records, to include records of emails sent and received, cell site location data, and a person's website browsing history—all without any court approval or independent oversight.

In addition, this bill report asserts that "certain providers" noncompliance is substantially impairing the FBI's ability to conduct national security investigations." Leaving aside the question of whether adherence to the law equates to 'noncompliance,' the FBI has merely stated, but not yet made a convincing case, that its conduct of national security investigations has been harmed by its inability to access ECTRs via National Security Letters.

Even as other committees in the Senate are working on ECPA reform legislation in open hearings, we should not be marking up a bill behind closed doors that makes a major change to existing statute without public discussion and debate.

We are also concerned about Section 603, which would narrow the oversight responsibilities of the Privacy and Civil Liberties Oversight Board (PCLOB). In additional views we submitted to the FY 2016 Intelligence Authorization Act report, we noted that we did not look favorably on a provision in the House-passed FY 2016 bill that would restrict PCLOB's mandate. Unfortunately, that provision became law. This year, it is the Senate bill that seeks to further constrain this small but important organization.

The PCLOB is the only independent, cross-government agency charged specifically with ensuring that the government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. Section 603 of the Intelligence Authorization Act would limit the authority of the PCLOB by narrowing its authority to review government programs to only those that impact the privacy and civil liberties of U.S. persons.

While the PCLOB already focuses primarily on U.S. persons, it is not mandated to do so exclusively. Limiting the PCLOB's mandate to only U.S. persons could create ambiguity about the scope of the PCLOB's mandate, raising questions in particular about how the PCLOB should proceed in the digital domain, where individuals' U.S. or non-U.S. status is not always apparent. It is conceivable, for example, that under this restriction, the PCLOB could not have reviewed the NSA's Section 702 surveillance program, which focuses on the communications of foreigners located outside of the United States, but which is also acknowledged to be incidentally collecting Americans' communications in the process.

The PCLOB is a small body, created as part of the Implementing Regulations of the 9/11 Commission Act of 2007 without any authority to implement its recommendations. However small, the PCLOB's creation recognized that the challenges of balancing privacy and civil liberties with our national security would only increase as our world becomes smaller due to the proliferation of new types of communication and other global interconnections.

The PCLOB has two fundamental responsibilities. First, it is charged with reviewing and analyzing executive branch counterterrorism actions to ensure that the actions our government take appropriately protect privacy and civil liberties. Second, it is charged with making sure that privacy and civil liberty protections are considered in the development of our counter-terrorism policies. In the post-9/11 world we live in, the PCLOB provides a critical voice within the executive branch that helps shape how our nation conducts itself as we contend with global terrorism and other challenges. Yet for the second year in a row, Congress would be narrowing PCLOB's jurisdiction. We believe this is not the right message to send.

MARTIN HEINRICH.
MAZIE K. HIRONO.

MINORITY VIEWS OF SENATOR WYDEN

While I respect the effort that my colleagues have put into drafting this year's Intelligence Authorization Act, I opposed this bill because it would dramatically and unnecessarily expand government surveillance authorities, and would undermine independent oversight of America's intelligence agencies.

National Security Letters

Specifically, this bill contains language—section 803—that would authorize individual Federal Bureau of Investigation (FBI) field offices to demand Americans' email and Internet records simply by issuing a National Security Letter, with no court oversight whatsoever.

This authority currently exists for phone records, and FBI officials have repeatedly suggested that it would be convenient if 'electronic communication transaction records,' such as email and Internet records, could be collected in the same way. But convenience alone does not justify such a dramatic erosion of Americans' constitutional rights.

If FBI officials have reason to suspect that an individual is connected to terrorism or espionage, they can already access that person's email and Internet records by simply obtaining an order from the Foreign Intelligence Surveillance Court. These orders can be issued in secret, and require relatively little evidence—the FBI simply needs to assert that the records are "relevant to an investigation." But requiring the approval of an independent judge provides an important check against the abuse or misuse of this authority by the FBI. By contrast, National Security Letters are not reviewed by a judge unless a company that receives one attempts to challenge it.

I certainly appreciate the FBI's interest in obtaining records about potential suspects quickly. But Foreign Intelligence Surveillance Court judges are very capable of reviewing and approving requests for court orders in a timely fashion. And section 102 of the recently-passed USA FREEDOM Act gives the FBI new authority to obtain records immediately in emergency situations, and then seek court review after the fact. I strongly supported the passage of that provision, which I first proposed in 2013. By contrast, I do not believe it is appropriate to give the government broad new surveillance authorities just because FBI officials do not like doing paperwork. If the FBI's own process for requesting court orders is too slow, then the appropriate solution is bureaucratic reforms, not a major expansion of government surveillance authorities.

While this bill does not clearly define 'electronic communication transaction records,' this term could easily be read to encompass records of whom individuals exchange emails with and when, as well as well as individuals' login history, IP addresses, and Inter-

net browsing history. This sort of surveillance can clearly reveal a great deal of personal information about individual Americans. Our Founding Fathers rightly argued that such intrusive searches should be approved by independent judges.

It is worth noting that President George W. Bush's administration reached the same conclusion. In November 2008, the Justice Department's Office of Legal Counsel advised the FBI that National Security Letters could only be used to obtain certain types of records, and this list did not include electronic communication transaction records. The FBI has unfortunately not adhered to this guidance, and has at times continued to issue National Security Letters for electronic communications records. A number of companies that have received these overly broad National Security Letters have rightly challenged them as improper. Broadening the National Security Letter law to include electronic communication transaction records would be a significant expansion of the FBI's statutory authority.

And unfortunately, the FBI's track record with its existing National Security Letter authorities includes a substantial amount of abuse and misuse. These problems have been extensively documented in reports by the Justice Department Inspector General from 2007, 2008, 2010 and 2014, so I will not repeat the details of these reports here. In my judgment, it would be reckless to expand this particular surveillance authority when the FBI has so frequently failed to use its existing authorities responsibly.

Privacy and Civil Liberties Oversight Board

Separately, I am troubled that this bill would erode the jurisdiction of the independent Privacy and Civil Liberties Oversight Board, for the second year in a row.

Specifically, the bill would narrow the Board's statutory jurisdiction to cover only programs that impact the privacy and civil liberties of U.S. persons. To date, the Board's oversight has focused very much on U.S. persons, and in my judgment this is entirely appropriate. But if the Intelligence Committee simply wanted to encourage the Board to maintain this focus, that could be accomplished with non-binding report language. Instead, this provision amends the law to limit the Board's official purview.

This is concerning because in the digital domain, individuals' U.S. or non-U.S. status is not always readily apparent, and restricting the Board in this way could discourage or even prevent the Board from examining programs whose impact on U.S. persons is not clear at first glance.

Additionally, while I support the Board's current focus on U.S. persons, it is easy to envision situations in which tasking the Board to produce a one-time report that also looked at non-U.S. persons might be appropriate. This provision would arguably prohibit the Board from taking on such projects.

Furthermore, I would note that over the past few years the Executive Branch has made real efforts to mitigate the diplomatic and economic damage that overly broad surveillance activities have caused. These efforts continue to be a work in progress, and foreign regulators continue to raise concerns about U.S. surveillance as justification for opposing agreements that would benefit American

consumers and the U.S. tech industry. I am therefore concerned that narrowing the Board's jurisdiction and signaling that the U.S. has no regard for the privacy of other countries' citizens would play into the hands of foreign protectionists.

Finally, I am troubled by the message that the Intelligence Committee is sending by supporting this provision. Over the past three years, the Privacy and Civil Liberties Oversight Board has done outstanding and highly professional work. It has examined large, complex surveillance programs and evaluated them in detail, and it has produced public reports and recommendations that are quite comprehensive and useful. Indeed, the Board's reports on major surveillance programs are the most thorough publicly available documents on this topic. My concern is that by acting to restrict the Board's purview for the second year in a row, and by making unwarranted criticisms of the Board's staff in this report, the Intelligence Committee is sending the message that the Board should not do its job too well.

Unfortunately, while I appreciate that this bill includes a proposal that I and a bipartisan, bicameral group of colleagues have put forward to allow the Board to hire staff even when the Board's chair position is vacant, the inclusion of this provision does not outweigh my substantial concerns with this bill.

I will continue to oppose this bill as long as the objectionable provisions noted above are included. I hope to be able to work with colleagues to remove these provisions prior to consideration of the bill by the full Senate. My further additional views on provisions contained in the classified annex to this bill can be found in the annex itself.

RON WYDEN.

○