**Calendar No. 207**

115TH CONGRESS, *1st Session* | SENATE | REPORT 115–151

# INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2018

SEPTEMBER 7, 2017.—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. 1761]

The Select Committee on Intelligence, having considered an original bill (S. 1761) to authorize appropriations for fiscal year 2018 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 June 12, 2017, 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 2018 is $57.7 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 2018 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 2018.

*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 2018 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. Personnel ceiling adjustments*

Section 103 provides that the DNI may authorize employment of civilian personnel in Fiscal Year 2018 in excess of the number of authorized positions by an amount not exceeding three percent of the total limit applicable to each Intelligence Community (IC) element under Section 102, and ten percent of the number of civilian personnel authorized under such schedule for the purposes of contractor conversions. The DNI may do so only if necessary to the performance of important intelligence functions.

*Section 104. Intelligence Community Management Account*

Section 104 authorizes appropriations in the amount of $550,200,000 for the Intelligence Community Management Account (ICMA) of the Office of the Director of National Intelligence (ODNI) for the elements within the ICMA for Fiscal Year 2018.

### 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 the Central Intelligence Agency Retirement and Disability Fund for Fiscal Year 2018.

### 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. Modification of special pay authority for science, technology, engineering, or mathematics positions and addition of special pay authority for cyber positions*

Section 303 provides an increased yearly cap for Science, Technology, Engineering, or Mathematics (STEM) employee positions in the IC who perform critical cyber missions.

*Section 304. Director of National Intelligence review of placement of positions within the intelligence community on the Executive Schedule*

Section 304 requires the DNI to conduct a review of the positions within the IC that may be appropriate for inclusion on the Executive Schedule, and the appropriate levels for inclusion.

*Section 305. Modification of appointment of Chief Information Officer of the Intelligence Community*

Section 305 changes the position of IC Chief Information Officer from being subject to presidential appointment to being subject to appointment by the DNI.

*Section 306. Supply Chain and Counterintelligence Risk Management Task Force*

Section 306 requires the DNI to establish a task force to standardize information sharing between the IC and the United States Government acquisition community with respect to supply chain and counterintelligence risks. Section 306 further provides requirements for membership, security clearances, and annual reports.

*Section 307. Inspector General of the Intelligence Community auditing authority*

Section 307 permits the IC IG to hire contractor or expert auditors to meet audit requirements, similar to other Federal IGs. Section 307 responds to the Committee's concerns that the IC Inspector General (IC IG) is at risk of failing to meet its legislative requirements due to its inability to hire qualified auditors by granting the IC IG independent hiring practices identical to other IGs.

*Section 308. Inspectors General studies on classification*

Section 308 requires each designated IG to carry out and submit to the congressional intelligence committees a report on the application of classification and handling markings on a representative sample of finished products, to include compartments. Section 308 also directs an analysis of compliance with declassification procedures and a review of the process for identifying topics of public or

historical importance that merit prioritization for declassification review.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

*Section 401. Authority for the protection of current and former employees of the Office of the Director of National Intelligence*

Section 401 amends Title 50, section 3506, to provide protection for current and former ODNI personnel and designated immediate family members, if there is a national security threat that warrants such protection.

*Section 402. Information sharing with State election officials*

Section 402 requires the DNI, within 30 days of enactment, to sponsor a security clearance for each eligible chief election official of a State, territory, or the District of Columbia (and up to one eligible designee), up to the top secret level. Section 402 also requires the DNI to share appropriate classified information-related threats to election systems and to the integrity of the election process with chief election officials and their designees who possess the aforementioned security clearances.

*Section 403. Technical modification to the Executive Schedule*

Section 403 amends Title 50, section 5313, to add the Director of the National Counterintelligence and Security Center.

*Section 404. Modification to the designation of the program manager-information sharing environment*

Section 404 changes the status of the Program Manager for the Information Sharing Environment from being subject to presidential appointment to being subject to appointment by the DNI.

Subtitle B—Other Elements

*Section 411. Repeal of foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency*

Section 411 repeals Title 50, section 3036(g), with conforming amendments to section 611 of the Intelligence Authorization Act for Fiscal Year 2005 (Public Law 108–487).

Subtitle C—Other Elements

*Section 421. Designation of the Counterintelligence Directorate of the Defense Security Service as an element of the intelligence community*

Section 421 adds the Defense Security Service's (DSS's) Counterintelligence (CI) Directorate to the IC elements in 50 U.S.C. 3003(4), and requires all IC requirements that apply to IC elements to apply to the DSS CI as of the date of enactment.

TITLE V—SECURING ENERGY INFRASTRUCTURE

*Section 501. Short title*

Section 501 provides that this title may be cited as the "Securing Energy Infrastructure Act of 2017."

*Section 502. Definitions*

Section 502 provides the relevant definitions as cited throughout this title.

*Section 503. Pilot program for securing energy infrastructure*

Section 503 requires the Director of Intelligence and Counterintelligence of the Department of Energy (hereinafter in this title, "Director"), within 180 days of enactment, to establish a two-year control systems implementation pilot program within the National Labs. This pilot program will partner with covered entities in the energy sector to identify new security vulnerabilities, and for purposes of researching, developing, testing, and implementing technology platforms and standards in partnership with such entities.

*Section 504. Working group to evaluate program standards and develop strategy*

Section 504 requires the Director to establish a working group composed of identified private and public sector entities, to evaluate the technology platforms and standards for the pilot program specified in Section 503 and develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities.

*Section 505. Reports on the program*

Section 505 requires the Director within 180 days after the date on which funds are first disbursed to submit to the congressional intelligence committees, the Committee on Energy and Natural Resources of the Senate, and the Committee on Energy and Commerce of the House of Representatives, an interim report that describes the pilot program's results, provides a feasibility analysis, and describes the working group's evaluations. Section 505 further requires the Director, within two years of funding, to submit to the aforementioned committees a progress report on the pilot program specified in Section 503, an analysis of the feasibility of the methods studied, and a description of the working group's evaluation results.

*Section 506. No new regulatory authority for Federal agencies*

Section 506 provides that nothing in this title permits the Director or the head of any other Federal agency to issue new regulations.

*Section 507. Exemption from disclosure*

Section 507 provides that information shared by or with the Federal Government or a State, tribal, or local government under this title shall be deemed to be voluntarily shared and exempt from disclosure under relevant laws requiring such disclosure.

*Section 508. Protection from liability*

Section 508 provides covered entities participating in the pilot program with protection from causes of action. Section 508 further provides that covered entities cannot be subject to causes of action for refraining from participation.

*Section 509. Authorization of appropriations*

Section 509 authorizes $10,000,000 to carry out the pilot program specified in Section 503, and $1,500,000 to carry out the working group and reporting provisions.

TITLE VI—REPORTS AND OTHER MATTERS

*Section 601. Technical correction to Inspector General study*

Section 601 amends Title 50, section 11001(d), by replacing the IC IG's "audit" requirement for Inspectors General with employees having classified material access, with a "review" requirement.

*Section 602. Governance for security clearance, suitability and fitness for employment, and credentialing*

Section 602 establishes an interagency council comprised of representatives from the ODNI, Office of Management and Budget, Office of Personnel Management, Under Secretary of Defense for Intelligence, and National Background Investigation Bureau, to govern decisions and processes related to security clearances, suitability and fitness for employment, and credentialing. Section 602 further establishes the DNI as the government's Security Executive Agent and the Director of the Officer of Personnel Management as the government's Suitability Executive Agent and the Credentialing Executive Agent, specifying roles and responsibilities for each.

*Section 603. Process for security clearances*

Section 603 incorporates several provisions relating to the security clearance process. Section 603 requires the following reviews: of the alignment among the Standard Form 86 background investigation questionnaire, the Federal Investigative Standards, and the adjudicative guidelines contained in Security Executive Agent Directive 4 ("National Security Adjudicative Guidelines"), as well as their collective utility in anticipating future insider threats; of certain methods to improve the background investigation process; and of the utility of the timelines for processing security clearances, as contained in the Intelligence Reform and Terrorism Prevention Act of 2004.

Section 603 also directs the DNI, as the government's Security Executive Agent, to establish a policy on the issuance of interim security clearances; establish a policy for consistent treatment in the security clearance process between government and contractor personnel; issue a strategy and implementation plan for conducting periodic reinvestigations based on risk, not a specified time interval; issue a policy for the government's use of automated records checks conducted for prior employment purposes; and establish a policy and issue an implementation plan for sharing information between and among government agencies and industry related to security clearances, consistent with privacy concerns.

*Section 604. Reports on the vulnerabilities equities policy and process of the Federal Government*

Section 604 requires the head of each IC element to submit within 90 days of enactment to the congressional intelligence committees a report detailing the process and criteria the head of each IC element uses for determining to submit a vulnerability for review under the Federal Government's vulnerabilities equities policy and process. Section 604 further requires the report to contain information about vulnerability disclosures to vendors, how many vulnerabilities have been patched, and when a patch or mitigation has been made publicly available.

*Section 605. Bug bounty programs*

Section 605 directs the Under Secretary for Intelligence and Analysis of the Department of Homeland Security to submit to congressional leadership and the congressional intelligence committees a strategic plan to implement bug bounty programs at appropriate agencies and departments of the United States Government. Section 605 further requires the plan to include an assessment of the "Hack the Pentagon" pilot program and subsequent bug bounty programs. Section 605 also requires the plan to provide recommendations on the feasibility of initiating bug bounty programs across the United States Government.

*Section 606. Report on cyber attacks by foreign governments against United States election infrastructure*

Section 606 directs the Under Secretary for Intelligence and Analysis of the Department of Homeland Security to submit to congressional leadership and the congressional intelligence committees a report on cyber attacks and attempted cyber attacks by foreign governments on United States election infrastructure, in connection with the 2016 Presidential election. Section 606 further requires this report to include identification of the States and localities affected and include efforts to attack voter registration databases, voting machines, voting-related computer networks, and the networks of secretaries of State and other election officials.

*Section 607. Review of intelligence community's posture to collect against and analyze Russian efforts to influence the presidential election*

Section 607 requires the DNI to submit to the congressional intelligence committees within one year of enactment a report on the Director's review of the IC's posture to collect against and analyze Russian efforts to interfere with the 2016 United States presidential election. Section 607 further requires the review to include assessments of IC resources, information sharing, and legal authorities.

*Section 608. Assessment of foreign intelligence threats to Federal elections*

Section 608 requires the DNI, in coordination with the Director of the CIA, the Director of the NSA, the Director of the FBI, the Secretary of Homeland Security, and the heads of other relevant IC elements, to commence assessments of security vulnerabilities of State election systems one year before regularly scheduled Federal

elections. Section 608 further requires the DNI to submit a report on such assessments to congressional leadership and to the congressional intelligence committees 180 days before regularly scheduled Federal elections, and an updated assessment 90 days before regularly scheduled Federal election.

*Section 609. Strategy for countering Russian cyber threats to United States elections*

Section 609 requires the DNI, in coordination with the Secretary of Homeland Security, the Director of FBI, the Director of CIA, the Secretary of State, the Secretary of Defense, and the Secretary of the Treasury, to develop a whole-of-government strategy for countering Russian cyber threats against United States electoral systems and processes. Section 609 further requires this strategy to include input from solicited Secretaries of State and chief election officials. Section 609 requires the DNI and the Secretary of Homeland Security to brief the congressional intelligence committees on the required strategy within 90 days of enactment.

*Section 610. Limitation relating to establishment or support of cyber security unit with the Government of Russia*

Section 610 prohibits the Federal Government from expending any funds to establish or support a cybersecurity unit or other cyber agreement that is jointly established or otherwise implemented by the United States Government and the Russian Government, unless the DNI submits a report to the congressional intelligence committees at least 30 days prior to any such agreement. The report shall include the agreement's purpose, intended shared intelligence, value to national security, counterintelligence concerns, and any measures taken to mitigate such concerns.

*Section 611. Report on returning Russian compounds*

Section 611 requires the IC to produce, within 180 days of enactment of this Act, both classified and unclassified reports on the intelligence risks of returning the two diplomatic compounds—one in New York and one in Maryland—taken from Russia as a reprisal for Russian meddling in the 2016 United States presidential election. Section 611 also establishes an ongoing requirement for producing similar assessments for future assignment of diplomatic compounds within the United States.

*Section 612. Intelligence community assessment on threat of Russian money laundering to the United States*

Section 612 requires the DNI, in coordination with the Secretary of the Treasury, to submit to the congressional intelligence committees within 180 days of enactment an IC assessment on the threat of Russian money laundering to the United States. Section 612 requires the assessment to be based on all-source intelligence from both the IC and the Office of Terrorism and Financial Intelligence of the Treasury Department and cover global nodes and entry points; vulnerabilities; connections between oligarchs, organized crime, and/or the Russian Government; counterintelligence threats to the United States; and challenges to United States Government efforts to enforce sanctions and combat organized crime.

*Section 613. Notification of an active measures campaign*

Section 613 requires the DNI to notify the Chairman and Vice Chairman or Ranking Member of the congressional intelligence committees each time the DNI has determined there is credible information that a foreign power has, is, or will attempt to employ a covert influence or active measures campaign with regard to the modernization, employment, doctrine, or force posture of the nuclear deterrent or missile defense. Section 613 further requires that such notification must include information about the actions that the United States has taken to expose or halt such attempts.

*Section 614. Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States*

Section 614 requires the Secretary of State, in executing the advance notification requirements of the Intelligence Authorization Act for Fiscal Year 2017, to ensure the Russian Federation provides two business days of advance notice to the Secretary prior to Russian diplomatic or consular travel, and to ensure that the Secretary provides further notification of this travel within one hour to the DNI and the Director of the Federal Bureau of Investigation.

*Section 615. Modification of certain reporting requirement on travel of foreign diplomats*

Section 615 amends a provision in the Intelligence Authorization Act for Fiscal Year 2017, to require reporting of "a best estimate" of known or suspected violations of certain travel requirements by accredited diplomatic and consular personnel of the Russian Federation.

*Section 616. Semiannual report on referrals to Department of Justice by elements of the intelligence community regarding unauthorized disclosure of classified information*

Section 616 requires the Assistant Attorney General of the Department of Justice, in consultation with the Director of the FBI, to submit to the congressional intelligence committees a semiannual report on the status of IC referrals to the Department regarding unauthorized disclosures of classified information.

*Section 617. Notifications on designation of an intelligence officer as a persona non grata*

Section 617 requires the DNI, in consultation with the Secretary of State, to submit to the congressional intelligence committees a notification within 30 days of an intelligence officer—either of the United States or of a foreign intelligence service stationed in the United States—being designated as a persona non grata. Section 617 further requires the notifications to include the basis for the designation and a justification for the expulsion.

*Section 618. Biennial report on foreign investment risks*

Section 618 requires the DNI to establish an IC working group on foreign investment risks and prepare a biennial report to the congressional intelligence committees. Section 618 further requires the report to include an identification, analysis, and explanation of national security vulnerabilities, foreign investment trends, foreign

countries' strategies to exploit vulnerabilities, and market distortions caused by foreign countries.

*Section 619. Report on surveillance by foreign governments against United States telecommunications networks*

Section 619 requires the DNI, in coordination with the Director of the CIA, the Director of the NSA, the Director of the FBI, and the Secretary of Homeland Security, to submit to the congressional intelligence committees within 180 days of enactment a report on known attempts by foreign governments to exploit cybersecurity vulnerabilities in United States telecommunications networks to target for surveillance United States persons, and any actions that the IC has taken to protect United States Government agencies and personnel from such surveillance.

*Section 620. Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security*

Section 620 requires the Secretary of Homeland Security, in consultation with the Under Secretary for Intelligence and Analysis, to submit to the congressional intelligence committees a report on the adequacy of the Under Secretary's authorities required as the Chief Intelligence Officer to organize the Homeland Security Intelligence Enterprise, and the legal and policy changes necessary to coordinate, organize, and lead Department of Homeland Security intelligence activities.

*Section 621. Report on geospatial commercial activities for basic and applied research and development*

Section 621 requires the Director of the National Geospatial-Intelligence Agency to submit, within 30 days of enactment, to the congressional intelligence committees and the armed services committees a report on the authorities that the Director deems necessary to conduct certain commercial activities to engage in specified basic and applied research, data transfers, and development projects. This report should address how the Director would use such authorities, consistent with applicable laws and procedures to protect sources and methods.

*Section 622. Technical amendments related to the Department of Energy*

Section 622 provides technical corrections to certain provisions regarding the Department of Energy's Office of Intelligence and Counterintelligence.

*Section 623. Sense of Congress on WikiLeaks*

Section 623 provides a Sense of Congress that WikiLeaks and its senior leadership resemble a non-state hostile intelligence service, often abetted by state actors, and should be treated as such.

## COMMITTEE COMMENTS

*Management of intelligence community workforce*

The Committee repeats direction from the Intelligence Authorization Act for Fiscal Year 2017 that IC elements should build, develop, and maintain a workforce appropriately balanced among its

civilian, military, and contractor workforce sectors to meet the missions assigned to it in law and by the president. Starting in fiscal year 2019, the Committee will no longer authorize position ceiling levels in the annual Schedule of Authorizations.

The bill, in Section 103, again includes authority for IC elements to adjust personnel ceilings by three percent, and by ten percent specifically for the purposes of contractor conversions. These flexibilities are temporary management tools to optimize the workforce this year that will cease in fiscal year 2019 when the IC can benefit from full implementation of the multi-sector workforce initiative.

The Committee looks forward to working with the ODNI as it develops an implementation strategy and sets standards for workforce cost analysis tools.

*Protection of the supply chain in intelligence community acquisition decisions*

The Committee continues to have significant concerns about risks to the supply chain in IC acquisitions. The report to accompany the Intelligence Authorization Act for Fiscal Year 2017 directed the DNI to review and consider changes to Intelligence Community Directive (ICD) 801 ("Acquisition") to reflect issuance in 2013 of ICD 731 ("Supply Chain Risk Management") and issues associated with cybersecurity. It specifically recommended the review examine whether to: expand risk management criteria in the acquisition process to include cyber and supply chain threats; require counterintelligence and security assessments as part of the acquisition and procurement process; propose and adopt new education requirements for acquisition professionals on cyber and supply chain threats; and factor in the cost of cyber and supply chain security. This review is due in November 2017, with a report on the process for updating ICD 801 due in December 2017.

As part of this review, the Committee directs three other considerations to be addressed: changes in the Federal Acquisition Regulation that may be necessary; how changes should apply to all acquisition programs; and how security risks must be addressed across development, procurement, and operational phases of acquisition. The Committee further directs the DNI to submit a plan to implement necessary changes within 60 days of completion of this review.

*National Geospatial-Intelligence Agency use of VERA and VSIP Authorities*

The Committee encourages the use by the National Geospatial-Intelligence Agency (NGA) of Voluntary Early Retirement Authority (VERA) and Voluntary Separation Incentive Program (VSIP) offers to meet its future goals of building a workforce more attuned to automation of data production, automation of analytic processes, and establishment of development and operations ("DevOps") software development processes.

Therefore, the Committee directs the NGA to report to the congressional intelligence committees within 120 days of enactment of this Act on its plan for further use of VERA and VSIP incentives, to include how they can be used to develop an acquisition cadre skilled in "DevOps" software development processes. The report should specify metrics for retooling its workforce, including how it

measures data literacy and computational skills in potential hires, and an accounting of the numbers of new hires who have met these higher standards.

*Report on engagement of National Reconnaissance Office with university community*

The Committee recognizes that the survivability and resiliency of United States satellites is critically important to the United States intelligence and defense communities. While the National Reconnaissance Office (NRO) engages with the university community in support of basic research and developing an education workforce pipeline to help advance new technologies and produce skilled professionals, it can do more in this regard to focus on space survivability.

Therefore, the Committee directs the NRO to report within 120 days of enactment of this Act on NRO's current efforts and future strategies to engage with university partners that are strategically located, host secure information facilities, and offer a strong engineering curriculum, with a particular focus on space survivability and resiliency. This report should provide a summary of NRO's current and planned university engagement programs, levels of funding, and program research and workforce objectives and metrics. The report should also include an assessment of the strategic utility of chartering a University Affiliated Research Center (UARC) in this domain.

*Clarification of oversight responsibilities*

The Committee reinforces the requirement for all IC agencies funded by the National Intelligence Program to respond in a full, complete, and timely manner to any request made by a member of the congressional intelligence committees. In addition, the Committee directs the DNI to issue guidelines within 90 days to ensure that this provision is carried out.

*Clarification on cooperation with investigation on Russian influence in the 2016 election*

The Committee reinforces the obligation for all IC agencies to cooperate in a full, complete, and timely manner with the Committee's investigation into Russian meddling in the 2016 Presidential election and all related inquiries being conducted by the Committee.

*Supervisory feedback as part of continuous evaluation program*

The Committee directs the DNI to review the results of ongoing pilots regarding the use of supervisory feedback as part of the periodic reinvestigation and continuous evaluation process and report within 180 days of enactment of this Act on the establishment of a policy for its use across the IC.

*National security threats to critical infrastructure*

The Committee is aware of significant threats to our critical infrastructure and industrial control systems posed by foreign adversaries. The sensitive nature of the information related to these threats make the role of the IC of vital importance to United States defensive efforts. The Committee has grave concerns that current

IC resources dedicated to these threats and their analysis are neither sufficient nor closely coordinated. The Committee includes provisions within this legislation to address these concerns.

*Inspector General of the Intelligence Community role and responsibilities*

The Inspector General of the Intelligence Community (IC IG) was established by the Intelligence Authorization Act for Fiscal Year 2010 to initiate and "conduct independent reviews investigations, inspections, audits, and reviews on programs and activities within the responsibility and authority of the Director of National Intelligence" and to lead the IG community in its activities. The Committee is concerned that this intent is not fully exercised by the IC IG and reiterates the Congress's intent that it consider its role as an IG over all IC-wide activities in addition to the ODNI. To support this intent, the Committee has directed a number of requirements to strengthen the IC IG's role and expects full cooperation from all Offices of Inspector General across the IC.

The Committee remains concerned about the level of protection afforded to whistleblowers within the IC and the level of insight congressional committees have into their disclosures. It is the Committee's expectation that all Offices of Inspector General across the IC will fully cooperate with the direction provided elsewhere in the bill to ensure both the Director of National Intelligence and the congressional committees have more complete awareness of the disclosures made to any IG about any National Intelligence Program funded activity.

*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, and encourages planned launches such as the U.S. Air Force Orbital/Sub-Orbital Program (OSP)-3 National Reconnaissance Office (NRO–111) mission, to be launched in 2018 on a Minotaur 1 from the Mid-Atlantic Regional Spaceport at Wallops Flight Facility. In the Fiscal Year 2017 Intelligence Authorization Act, the Committee directed a brief from the ODNI, in consultation with the Department of Defense and the U.S. Air Force, on their plans to utilize state-owned and operated spaceports, which leverage non-federal public and private investments to bolster United States launch capabilities and provide access to mid-to-low or polar-to-high inclination orbits for national security missions.

The Committee directs that the ODNI supplement this brief to consider how state investments in these spaceports may support infrastructure improvements, such as payload integration and launch capabilities, for national security launches.

## COMMITTEE ACTION

On July 27, 2017, 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 eight amendments to the classified annex, as sponsored by: (1) Chairman Burr and Vice Chairman Warner, as modified by a second-degree amendment by Chairman Burr and Senator Cotton; (2) Chairman Burr and Vice Chairman Warner; (3) Chairman Burr and Vice Chairman Warner; (4) Vice Chairman Warner and Senator Manchin; (5) Senator Manchin, as modified by a second-degree amendment by Chairman Burr; (6) Senator Lankford, as modified by a second-degree amendment by Senator Lankford and Vice Chairman Warner; (7) Senator Rubio, as modified by a second-degree amendment also by Senator Rubio; and (8) Senator Rubio, Senator Cornyn, and Senator Manchin.

By voice vote, the Committee adopted *en bloc* the following eleven amendments to the bill: (1) an amendment by Chairman Burr and Vice Chairman Warner to Section 505, regarding reports on an energy infrastructure pilot program; (2) an amendment by Vice Chairman Warner and Senator Heinrich, regarding Russia cyber threat strategy; (3) an amendment by Chairman Burr and Senator Rubio to Section 402, regarding information sharing with state election officials; (4) an amendment by Senator Collins, Senator Lankford, and Senator Manchin that requires the Department of Justice to report on Intelligence Community leaks; (5) an amendment by Senator Cotton that modifies a report requirement on certain Russia travel violations; (6) an amendment by Senator Heinrich, Senator King, and Senator Harris that requires reporting on the government's Vulnerabilities Equities Policy and Process; (7) an amendment by Senator Lankford to Section 608, regarding an assessment of foreign intelligence threats to federal elections; (8) an amendment by Senator Harris requiring an Intelligence Community review on Russian influence; (9) an amendment by Senator Wyden and Senator Manchin requiring a report on Russian money laundering; (10) an amendment by Senator Wyden prohibiting a United States-Russia cyber unit; and (11) an amendment by Senator Wyden requiring a report on foreign government surveillance against United States telecommunications networks.

By voice vote, the Committee adopted a second-degree amendment by Senator King to an amendment by Senator Wyden that would have stricken Section 623 of the bill. Section 623 originally provided a Sense of Congress that WikiLeaks and its senior leadership constitute a non-state hostile intelligence service.

By a vote of 13 ayes to 2 noes, the Committee adopted the amendment by Senator Wyden that would have stricken Section 623 of the bill, as modified by the second-degree amendment by Senator King, to provide a Sense of Congress that WikiLeaks and its senior leadership resemble a non-state hostile intelligence service. The votes in person or by proxy were as follows: Chairman Burr—aye; Senator Risch—aye; Senator Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Lankford—aye; Senator Cotton—aye; Senator Cornyn—aye; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—no; Senator Heinrich—

aye; Senator King—aye; Senator Manchin—aye; and Senator Harris—no.

Senator Feinstein offered an amendment regarding civil injunction actions and an amendment to require reports on terrorist activities, both of which she subsequently withdrew.

Senator Wyden offered an amendment regarding whistleblower protections for Intelligence Community contractors, which he subsequently withdrew.

Senator Cotton offered three amendments, which he subsequently withdrew, as follows: (1) an amendment to require a declassification review of materials relating to the Iran Joint Comprehensive Plan of Action; (2) an amendment to make a conforming edit to 18 U.S.C. 2709, to clarify that the government is permitted to obtain non-content electronic communications transactional records; and (3) an amendment to reauthorize Title VII of the Foreign Intelligence Surveillance Act.

*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 Rubio—aye; Senator Collins—aye; Senator Blunt—aye; Senator Lankford—aye; Senator Cotton—aye; Senator Cornyn—aye; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—no; Senator Heinrich—aye; Senator King—aye; Senator Manchin—aye; and Senator Harris—aye.

By unanimous consent, the Committee authorized the staff to make technical and conforming changes, 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 July 27, 2017, 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 regu-

latory impact will be incurred by implementing the provisions of this legislation.

## ADDITIONAL VIEWS OF SENATOR HARRIS

I support the Senate Select Committee on Intelligence's Fiscal Year 2018 Intelligence Authorization Act because it advances a number of important intelligence oversight goals ranging from transparency on cyber vulnerabilities to tracking foreign threats to our elections. Nevertheless, despite my overall support for the bill, it is not perfect.

In particular, I have reservations about Section 623, which establishes a Sense of Congress that WikiLeaks and the senior leadership of WikiLeaks resemble a non-state hostile intelligence service. The Committee's bill offers no definition of "non-state hostile intelligence service" to clarify what this term is and is not. Section 623 also directs the United States to treat WikiLeaks as such a service, without offering further clarity.

To be clear, I am no supporter of WikiLeaks, and believe that the organization and its leadership have done considerable harm to this country. This issue needs to be addressed. However, the ambiguity in the bill is dangerous because it fails to draw a bright line between WikiLeaks and legitimate journalistic organizations that play a vital role in our democracy.

I supported efforts to remove this language in Committee and look forward to working with my colleagues as the bill proceeds to address my concerns.

KAMALA D. HARRIS.

## MINORITY VIEWS OF SENATOR WYDEN

The Fiscal Year 2018 Intelligence Authorization bill includes three important amendments I offered.

The first amendment requires that the Director of National Intelligence, in coordination with the Secretary of the Treasury, produce a report on the threat to the United States from Russian money laundering. It has become apparent that following the trail of illicit Russian money is a central component of any counterintelligence investigation related to Russia. Russian money laundering also threatens the U.S. financial system as well as efforts to enforce sanctions and fight organized crime. This report will bring together the resources of the Intelligence Community and elements of the Treasury Department under the Office of Terrorism and Financial Intelligence, such as the Financial Crimes Enforcement Network (FinCEN), so that the government and the Congress can understand the complex and hidden networks of shell companies and other money laundering instruments overseas and here in the United States.

The second amendment prohibits the U.S.-Russia cyber security unit announced by the President on July 9, 2017, or any other U.S.-Russia cyber agreement, unless Congress has full information about what the administration intends. The President's statement that this unit will ensure that "election hacking, & many other negative things, will be guarded and safe" raises numerous counterintelligence concerns, given Russia's hacking in connection with the 2016 U.S. election. My amendment thus requires the DNI, at least 30 days prior to any such agreement, to report on what intelligence will be shared with Russia, the counterintelligence concerns associated with any such agreement, and what will be done to mitigate those concerns.

The third amendment requires a report on the threat that cyber security vulnerabilities in telecommunications networks, including Signaling System No. 7 (SS7), could result in foreign government surveillance of Americans, including U.S. government personnel. A Department of Homeland Security report from April highlighted the risks of SS7 vulnerabilities. My amendment will require the whole of the Intelligence Community to report on whether foreign government surveillance is occurring as a result of this known vulnerability, and what the IC is doing about it.

One important reform lacking from the bill is whistleblower protections for Intelligence Community contractors, who are not afforded the protections provided either to Intelligence Community employees or to contractors outside the Intelligence Community. By addressing this gap, Congress potentially could save the taxpayers millions of dollars. Extending whistleblower protections to IC contractors also helps discourage leaks by granting potential leakers protected classified channels to express concerns. It is my intent to

continue to work with colleagues to address this shortcoming in whistleblower protections in the near future.

My opposition to the bill is based on a provision stating that it is the Sense of Congress "that WikiLeaks and the senior leadership of WikiLeaks resemble a non-state hostile intelligence service often abetted by state actors and should be treated as such a service by the United States." My concern with this language does not relate to the actions of WikiLeaks, which, as I have stressed in the past, was part of a direct attack on our democracy. My concern is that the use of the novel phrase "non-state hostile intelligence service" may have legal, constitutional, and policy implications, particularly should it be applied to journalists inquiring about secrets. The language in the bill suggesting that the U.S. government has some unstated course of action against "non-state hostile intelligence services" is equally troubling.

The damage done by WikiLeaks to the United States is clear. But with any new challenge to our country, Congress ought not react in a manner that could have negative consequences, unforeseen or not, for our constitutional principles. The introduction of vague, undefined new categories of enemies constitutes such an ill-considered reaction.

RON WYDEN.

○