Calendar No. 494

115TH CONGRESS, *2d Session* | SENATE | REPORT 115–298

MATTHEW YOUNG POLLARD INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEARS 2018 AND 2019

JULY 11, 2018.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany S. 3153]

The Select Committee on Intelligence, having considered an original bill (S. 3153) to authorize appropriations for fiscal years 2018 and 2019 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

CLASSIFIED ANNEXES 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 was $57.7 billion. On February 27, 2018, acting pursuant to Section 364 of the Intelligence Authorization Act for Fiscal Year 2010 (Public Law 111–259), the DNI publicly disclosed that the President's aggregate request for the National Intelligence Program for Fiscal Year 2019 was $59.9 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 budg-

etary recommendations. Accordingly, the Committee has prepared classified annexes to this report that contain classified Schedules of Authorizations; one for Fiscal Year 2018, and one for Fiscal Year 2019. The classified annex and Schedule of Authorizations for Fiscal Year 2018 reflect negotiations with the House Permanent Select Committee on Intelligence for a joint explanatory statement and accompanying classified annex in anticipation of separate passage of an Intelligence Authorization Act for Fiscal Year 2018. The classified Schedules of Authorizations are incorporated by reference in the Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019 and have the legal status of public law. The classified annexes are made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President. They are also available for review by any Member of the Senate subject to 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 Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019 (the "Act") that was 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 and Fiscal Year 2019. Section 101 further clarifies that certain appropriated funds are authorized for purposes of Section 504 of the National Security Act of 1947 (50 U.S.C. 3094) and limits certain waivers for (1) activities authorized under Section 503 of the National Security Act of 1947 (50 U.S.C. 3093), and (2) major systems as defined in Section 506A(e) of the National Security Act of 1947 (50 U.S.C. 3097), unless the DNI notifies the congressional intelligence committees that the activities are urgent for national security purposes.

Section 102. Classified Schedules 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 and Fiscal Year 2019 are contained in classified Schedules of Authorizations and that the classified Schedules 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 con-

tractor conversions. The DNI may do so only if necessary to the performance of important intelligence functions. If the DNI exercises the provision allowing for contractor conversions, the DNI shall provide written justification to the congressional intelligence committees.

Section 103 does not authorize personnel for Fiscal Year 2019, given the congressional intelligence committees have committed to allowing the IC to manage by funding under its multisector workforce initiative, and no longer by positions.

Section 104. Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the ODNI for Fiscal Year 2018 and Fiscal Year 2019. Section 104 authorizes personnel for Fiscal Year 2018, but consistent with Section 103, Section 104 does not authorize personnel for Fiscal Year 2019, given the congressional intelligence committees have committed to allowing the IC to manage by funding under its multisector workforce initiative, and no longer by positions.

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 CIA Retirement and Disability Fund for each of Fiscal Years 2018 and 2019.

Section 202. Computation of annuities for employees of the Central Intelligence Agency

Section 202 makes technical changes to the CIA Retirement Act to conform with various statutes governing the Civil Service Retirement System.

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 that support critical cyber missions. Section 303 also per-

mits the National Security Agency (NSA) to establish a special rate of pay for positions that perform functions that execute the agency's cyber mission.

Section 304. Modification of appointment of Chief Information Officer of the Intelligence Community

Section 304 changes the position of IC Chief Information Officer from being subject to presidential appointment to being subject to appointment by the DNI.

Section 305. Director of National Intelligence review of placement of positions within the intelligence community on the Executive Schedule

Section 305 requires the DNI, in coordination with the Office of Personnel Management, 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 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. Consideration of adversarial telecommunications and cybersecurity infrastructure when sharing intelligence with foreign governments and entities

Section 307 requires the IC, when entering into foreign intelligence sharing agreements, to consider the pervasiveness of telecommunications and cybersecurity infrastructure, equipment, and services provided by United States adversaries or entities thereof.

Section 308. Cyber protection support for the personnel of the intelligence community in positions highly vulnerable to cyber attack

Section 308 permits the DNI to provide cyber protection support for the personal technology devices and personal accounts of IC personnel whom the DNI determines to be highly vulnerable to cyber attacks and hostile information collection activities.

Section 309. Modification of authority relating to management of supply-chain risk

Section 309 extends certain IC procurement authorities to manage and protect against supply chain risks. Section 309 further requires annual reporting on the IC's determinations and notifications made in executing these authorities.

Section 310. Limitations on determinations regarding certain security classifications

Section 310 prohibits an officer of the IC who is nominated to a Senate-confirmed position from making certain classification determinations posing potential conflicts of interest regarding that nominee.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 401. Authority for 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. Designation of the Program Manager-Information Sharing Environment

Section 402 amends the Intelligence Reform and Terrorism Protection Act of 2004 so that the Program Manager-Information Sharing Environment (PM–ISE) is subject to appointment by the DNI, not the President.

Section 403. Modification to the Executive Schedule

Section 403 amends the Executive Schedule to make the Director of the National Counterintelligence and Security Center a Level IV position on the Executive Schedule.

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).

Section 412. Plan for designation of counterintelligence component of the Defense Security Service as an element of intelligence community

Section 412 directs the DNI and the Under Secretary of Defense for Intelligence, in coordination with the Director of the National Counterintelligence and Security Center, to provide the congressional intelligence and defense committees with an implementation plan to make the Defense Security Service's (DSS's) Counterintelligence component an element of the IC as defined in paragraph (4) of section 3 of the National Security Act of 1947 (50 U.S.C. 3003(4)), by January 1, 2020. Section 412 further provides that the plan shall not address the DSS's personnel security functions.

Section 413. Notice not required for private entities

Section 413 provides a Rule of Construction that the Secretary of the Department of Homeland Security (DHS) is not required to provide notice to private entities before issuing directives on agency information security policies and practices.

TITLE V—ELECTION MATTERS

Section 501. Report on cyber attacks by foreign governments against United States election infrastructure

Section 501 directs the Under Secretary for Intelligence and Analysis (I&A) of DHS to submit 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 501 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 502. Review of intelligence community's posture to collect against and analyze Russian efforts to influence the Presidential election

Section 502 requires the DNI to submit to the congressional intelligence committees, within one year of enactment of this Act, 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 502 further requires the review to include assessments of IC resources, information sharing, and legal authorities.

Section 503. Assessment of foreign intelligence threats to Federal elections

Section 503 requires the DNI, in coordination with the Director of the CIA, Director of the NSA, Director of the FBI, Secretary of DHS, and heads of other relevant IC elements, to commence assessments of security vulnerabilities of State election systems one year before regularly scheduled Federal elections. Section 503 further requires the DNI to submit a report on such assessments 180 days before regularly scheduled Federal elections, and an updated assessment 90 days before regularly scheduled Federal elections.

Section 504. Strategy for countering Russian cyber threats to United States elections

Section 504 requires the DNI, in coordination with the Secretary of DHS, Director of the FBI, Director of the CIA, Secretary of State, Secretary of Defense, and Secretary of the Treasury, to develop a whole-of-government strategy for countering Russian cyber threats against United States electoral systems and processes. Section 504 further requires this strategy to include input from solicited Secretaries of State and chief election officials.

Section 505. Information sharing with State election officials

Section 505 requires the DNI, within 30 days of enactment of this Act, to support the Under Secretary for I&A at DHS, and any other appropriate designees of the Secretary of DHS in sponsoring a security clearance for each eligible chief election official of a State, territory, or the District of Columbia (and additional eligible designees), up to the top secret level. Section 505 also requires the DNI to assist the Under Secretary for I&A with sharing appropriate classified information about 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 506. Designation of counterintelligence officer to lead election security matters

Section 506 requires the DNI to designate a national counterintelligence officer within the National Counterintelligence and Security Center to lead, manage, and coordinate election security-related counterintelligence matters, including certain risks from foreign power interference.

TITLE VI—SECURITY CLEARANCES

Section 601. Definitions

Section 601 provides definitions for terminology used throughout this Title.

Section 602. Reports and plans relating to security clearances and background investigations

Section 602 requires the interagency Performance Accountability Council (Council) to provide plans to reduce the background investigation inventory and best align the investigation function between the Department of Defense and the National Background Investigation Bureau. Section 602 further requires the Council to report on the future of the clearance process and requires the DNI to notify the appropriate committees upon determining requests to change clearance standards, and the status of those requests' disposition.

Section 603. Improving the process for security clearances

Section 603 requires the DNI to review the Questionnaire for National Security positions (SF–86) and the Federal Investigative Standards to determine potential unnecessary information required and assess whether revisions are necessary to account for insider threats. Section 603 further requires the DNI, in coordination with the Council, to establish policies on interim clearances and consistency between the clearance process for contract and government personnel.

Section 604. Goals for promptness of determinations regarding security clearances

Section 604 requires the Council to implement a plan to be able to process ninety percent of clearance requests at the Secret level in thirty days, and at the Top Secret level in ninety days. The plan shall also address how to recognize reciprocity in accepting clearances among agencies within two weeks, and to require that ninety percent of clearance holders not be subject to a time-based periodic investigation.

Section 605. Security Executive Agent

Section 605 establishes the DNI as the government's Security Executive Agent, consistent with Executive Order 13467, and sets forth relevant authorities.

Section 606. Report on unified, simplified, government-wide standards for positions of trust and security clearances

Section 606 directs the DNI and the Director of the Office of Personnel Management to report on the advisability and implications of consolidating the tiers for positions of trust and security clearances from five to three tiers.

Section 607. Report on clearance in person concept

Section 607 requires the DNI to submit a report on a concept whereby an individual can maintain eligibility for access to classified information for up to three years after access may lapse.

Section 608. Budget request documentation on funding for clearances

Section 608 requires the President to submit to Congress with the Fiscal Year 2020 budget request exhibits that identify resources allocated by each agency for processing security clearances, identified by each respective tier.

Section 609. Reports on reciprocity for security clearances inside of departments and agencies

Section 609 requires each federal agency to submit a report to the DNI that identifies the number of clearances that take more than two weeks to reciprocally recognize and set forth the reason for any delays. Section 609 further requires the DNI to submit an annual report summarizing reciprocity.

Section 610. Intelligence community reports on security clearances

Section 610 requires the DNI to submit a report on each IC element's security clearance metrics, segregated by Federal employees and contractor employees.

Section 611. Periodic report on positions in the intelligence community which can be conducted without access to classified information, networks, or facilities

Section 611 requires the DNI to submit to the congressional intelligence committees a report on positions that can be conducted without access to classified information, networks, or facilities, or may require only a secret-level clearance.

Section 612. Information sharing program for positions of trust

Section 612 requires the Security Executive Agent to establish a program to share information between and among government agencies and industry partners to inform decisions about positions of trust and security clearances.

Section 613. Report on protections for confidentiality of whistleblower-related communications

Section 613 requires the Security Executive Agent, in coordination with the Inspector General of the Intelligence Community, to submit a report detailing the IC's controls used to ensure continuous evaluation programs protect the confidentiality of whistleblower-related communications.

TITLE VII—REPORTS AND OTHER MATTERS

SUBTITLE A—MATTERS RELATING TO RUSSIA AND OTHER FOREIGN POWERS

Section 701. Limitation relating to establishment or support of cybersecurity unit with the Government of Russia

Section 701 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 and the armed services 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 702. Report on returning Russian compounds

Section 702 requires the IC to submit to the congressional intelligence committees, within 180 days of enactment of this Act, both classified and unclassified reports on the intelligence risks of returning the diplomatic compounds—in New York, Maryland, and California—taken from Russia as a reprisal for Russian meddling in the 2016 United States presidential election. Section 702 also establishes an ongoing requirement for producing similar assessments for future assignment of diplomatic compounds within the United States.

Section 703. Assessment of threat finance relating to Russia

Section 703 requires the DNI, in coordination with the Assistant Secretary of the Treasury for Intelligence and Analysis, to submit to the congressional intelligence committees, within 60 days of enactment of this Act, an assessment of Russian threat finance, based on all-source intelligence from both the IC and the Office of Terrorism and Financial Intelligence of the Treasury Department. Section 703 further requires the assessment to include global nodes and entry points for Russian money laundering; United States vulnerabilities; connections between Russian individuals involved in money laundering and the Russian Government; counterintelligence threats to the United States posed by Russian money laundering and other forms of threat finance; and challenges to United States Government efforts to enforce sanctions and combat organized crime.

Section 704. Notification of an active measures campaign

Section 704 requires the DNI to notify congressional leadership, and the Chairman and Vice Chairman or Ranking Member of the congressional intelligence committees and the armed services committees, each time the DNI has determined there is credible information that a foreign power has attempted, is attempting, 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 704 further requires that such notification must include information on

any actions that the United States has taken to expose or halt such attempts.

Section 705. Notification of travel by accredited diplomatic and consular personnel of the Russian Federation in the United States

Section 705 requires the Secretary of State to ensure that the Russian Federation provides notification at least two business days in advance of all travel that is subject to such requirements by accredited diplomatic and consular personnel of the Russian Federation in the United States, and take necessary action to secure full compliance by Russian personnel and address any noncompliance.

SUBTITLE B—REPORTS

Section 711. Technical correction to Inspector General study

Section 711 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 712. Reports on authorities of the Chief Intelligence Officer of the Department of Homeland Security

Section 712 requires the Secretary of DHS, in consultation with the Under Secretary for I&A, 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 DHS intelligence activities.

Section 713. Report on cyber exchange program

Section 713 directs the DNI to submit a report, within 90 days of enactment of this Act, on the potential establishment of a voluntary cyber exchange program between the IC and private technology companies.

Section 714. Report on role of Director of National Intelligence with respect to certain foreign investments

Section 714 directs the DNI to submit a report on ODNI's role in preparing analytic materials in connection with the United States Government's evaluation of national security risks associated with potential foreign investments.

Section 715. Report on surveillance by foreign governments against United States telecommunications networks

Section 715 requires the DNI, in coordination with the Director of the CIA, Director of the NSA, Director of the FBI, and Secretary of DHS, to submit to the congressional intelligence, judiciary, and homeland security committees, within 180 days of enactment of this Act, a report on known attempts by foreign governments to exploit cybersecurity vulnerabilities in United States telecommunications networks to surveil United States persons, and any actions that the IC has taken to protect United States Government agencies and personnel from such surveillance.

Section 716. Biennial report on foreign investment risks

Section 716 requires the DNI to establish an IC working group on foreign investment risks and prepare a biennial report that includes an identification, analysis, and explanation of national security vulnerabilities, foreign investment trends, foreign countries' strategies to exploit vulnerabilities through the acquisition of either critical technologies (including components or items essential to national defense), critical materials (including physical materials essential to national security), or critical infrastructure (including physical or virtual systems and assets whose destruction or incapacity would have a debilitating impact on national security), and market distortions caused by foreign countries. Technologies, materials, and infrastructure are deemed to be "critical" under this provision if their exploitation by a foreign government could cause severe harm to the national security of the United States.

Section 717. Modification of certain reporting requirement on travel of foreign diplomats

Section 717 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 718. Semiannual reports on investigations of unauthorized disclosures of classified information

Section 718 requires the Assistant Attorney General for National Security at the Department of Justice, in consultation with the Director of the FBI, to submit to the congressional intelligence and judiciary committees a semiannual report on the status of IC referrals to the Department regarding unauthorized disclosures of classified information. Section 718 also directs IC elements to submit to the congressional intelligence committees a semiannual report on the number of investigations opened and completed by each agency regarding an unauthorized public disclosure of classified information to the media, and the number of completed investigations referred to the Attorney General.

Section 719. Congressional notification of designation of covered intelligence officer as persona non grata

Section 719 requires, not later than 72 hours after a covered intelligence officer is designated as *persona non grata,* that the DNI, in consultation with the Secretary of State, submit to the congressional intelligence committees a notification of that designation, to include the basis for the designation and justification for the expulsion.

Section 720. Inspectors General reports on classification

Section 720 requires each designated IG to submit to the congressional intelligence committees a report on the accuracy in the application of classification and handling markings on a representative sample of finished products, to include those with compartments. Section 720 also directs analyses of compliance with declassification procedures and a review of the effectiveness of processes

for identifying topics of public or historical importance that merit prioritization for declassification review.

Section 721. Reports on intelligence community participation in vulnerabilities equities process of Federal Government

Section 721 requires the DNI to submit, within 90 days of enactment of this Act, to the congressional intelligence committees a report describing the Vulnerabilities Equities Process (VEP) roles and responsibilities for each IC element. Section 721 further requires each IC element to report to the congressional intelligence committees within 30 days of a significant change to that respective IC element's VEP process and criteria. Section 721 also requires the DNI to submit an annual report to the congressional intelligence committees with specified information on certain VEP metrics.

Section 722. Reports on global water insecurity and national security implications

Section 722 requires the DNI to submit to the congressional intelligence committees a report every five years on the implications of global water insecurity on the United States' national security interests.

Section 723. Annual report on memoranda of understanding between elements of intelligence community and other entities of the United States Government regarding significant operational activities or policy

Section 723 amends a provision in the *Intelligence Authorization Act for Fiscal Year 2017,* instead requiring each IC element to submit an annual report to the congressional intelligence committees that lists each significant memorandum of understanding or other agreement entered into during the preceding fiscal year. Section 723 further requires each IC element to provide such documents if an intelligence committee so requests.

Section 724. Repeal of report requirement for inspectors general of certain elements of intelligence community

Section 724 repeals an annual reporting requirement for Inspectors General of the NSA, DIA, NRO, and NGA, while leaving intact ongoing substantive semiannual reporting requirements for those Inspectors General.

Section 725. Repeal of requirement for annual personnel level assessments for the intelligence community

Section 725 repeals the DNI's requirement to provide an annual personnel level assessment for each IC element.

Section 726. Report on outreach strategy addressing threats from United States adversaries to the United States technology sector

Section 726 requires the DNI to submit a report to appropriate committees on the IC's and the Defense Intelligence Enterprise's (DIE's) outreach to United States non-government entities (including private businesses and academia), regarding the United States' adversaries' efforts to acquire critical United States infrastructure

technology, intellectual property, and research and development information.

Section 727. Study on the feasibility of encrypting unclassified wireline and wireless telephone calls

Section 727 requires the DNI to complete a study and report on the feasibility of encrypting unclassified wireline and wireless telephone calls between personnel in the IC.

Section 728. Modification of requirement for annual report on hiring and retention of minority employees

Section 728 expands and clarifies current IC reporting requirements on diversity of IC personnel to include five prior fiscal years and to disaggregate data by IC element.

SUBTITLE C—OTHER MATTERS

Section 731. Technical amendments related to the Department of Energy

Section 731 provides technical corrections to certain provisions regarding the Department of Energy's Office of Intelligence and Counterintelligence.

Section 732. Securing energy infrastructure

Section 732 requires the Secretary of Energy (hereinafter in this section, "Secretary"), within 180 days of enactment of this Act, to establish a two-year control systems implementation pilot program within the National Laboratories. 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 732 also requires the Secretary to establish a working group composed of identified private and public sector entities to evaluate the technology platforms and standards for the pilot program, and develop a national cyber-informed engineering strategy to isolate and defend covered entities from security vulnerabilities. Section 732 requires the Secretary, within 180 days after the date on which funds are first disbursed, to submit to specified committees an interim report that describes the pilot program's results, provides a feasibility analysis, and describes the working group's evaluations. Section 732 further requires the Secretary, within two years of funding, to submit to the aforementioned committees a progress report on the pilot program and an analysis of the feasibility of the methods studied, and a description of the working group's evaluation results.

Section 733. Sense of Congress on WikiLeaks

Section 733 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.

Section 734. Bug bounty programs

Section 734 directs the Secretary of DHS, in consultation with the Secretary of Defense, to submit a strategic plan to implement bug bounty programs at appropriate agencies and departments of

the United States Government. Section 734 further requires the plan to include an assessment of the "Hack the Pentagon" pilot program and subsequent bug bounty programs. Section 734 also requires the plan to provide recommendations on the feasibility of initiating bug bounty programs across the United States Government.

Section 735. Sense of Congress on consideration of espionage activities when considering whether or not to provide visas to foreign individuals to be accredited to a United Nations mission in the United States

Section 735 provides a Sense of Congress that, as to foreign individuals to be accredited to a United Nations mission, the Secretary of State should consider known and suspected intelligence and espionage activities, including activities constituting precursors to espionage, carried out by such individuals against the United States, or against foreign allies or partners of the United States. Section 735 further provides that the Secretary of State should consider an individual's status as a known or suspected intelligence officer for a foreign adversary.

Section 736. Extension of provisions relating to declassification of information in the public interest

Section 736 reauthorizes the Public Interest Declassification Board administered by the National Archives for a term of four years, expiring on December 31, 2022.

Section 737. Modification of authorities relating to the National Intelligence University

Section 737 provides the National Intelligence University with three authorities that certain other Department of Defense educational institutions have regarding hiring faculty, accepting research grants, and enrolling eligible private sector individuals.

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 if done for the purposes of contractor conversions. These flexibilities are temporary management tools to optimize the workforce this year that will cease in fiscal year 2020 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.

Authorization of appropriated funds

The Committee is committed to ensuring that section 504 of the National Security Act of 1947 (50 U.S.C. 3094) ("Section 504"), first enacted in the *Intelligence Authorization Act for Fiscal Year 1986,* is consistently upheld. Section 504 assures the American public that the congressional intelligence committees have reviewed and authorized funding appropriated for intelligence and intelligence related activities. While specific, temporary waivers of Section 504 may be required in extraordinary exigent circumstances, such temporary waivers remain subject to subsequent review and permanent authorization by the committees that Congress created for the specific purpose of overseeing U.S. intelligence activities. Activities authorized pursuant to section 503 of the National Security Act of 1947 (50 U.S.C. 3093) are of particular Committee interest. Therefore, the Committee will continue to ensure that any appropriation that affects activities within the Committees' jurisdiction shall be reviewed and authorized in full accordance with Section 504.

Countering Russian propaganda

The Committee supports the IC's role in countering Russian propaganda and other active measures. The Committee is committed to providing the appropriate legal authorities, financial resources, and personnel necessary to address these hostile acts. The Committee specifically finds that language capabilities are important to the IC's efforts in countering Russia's hostile acts. The Committee encourages the IC to commit considerable resources in the future to bolstering officers' existing Russian language skills, recruiting Russian language speakers, and training officers in Russian, in particular key technical language skills. This effort will require strategic planning both in recruiting and rotating officers through language training. The Committee expects to see these priorities reflected in future IC budget requests.

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 was due in November 2017, with a report on the process for updating ICD 801 in December 2017. The report was completed on June 18, 2018.

As a follow-on to 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 use to date of VERA and VSIP incentives, to include how they have been used to develop an acquisition cadre skilled in "DevOps"' software development processes, as well as a plan for further use of these incentives. 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.

National Geospatial-Intelligence Agency Facilities

Consistent with Section 2401 of the National Defense Authorization Act for Fiscal Year 2018, the Committee authorizes the President's request for $381 million in Fiscal Year 2018 for phase one construction activities. The Committee recommends $447.8 million in Fiscal Year 2019 for phase two construction activities of the Next National Geospatial-Intelligence Agency (NGA) West (N2W) facility in St. Louis, Missouri. The Committee is pleased that the

second phase of this $837.2 million project is included in the Fiscal Year 2019 President's budget.

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 for information made by a member of the congressional intelligence committees. In addition, the Committee directs the DNI to issue guidelines, within 90 days of enactment of this Act, to ensure that the intent of Section 501 of the National Security Act of 1947 (50 U.S.C. 3091) is carried out.

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

The Committee continues to reinforce the obligation for all IC agencies to cooperate in a full, complete, and timely manner with the Committee's ongoing investigation into Russian meddling in the 2016 Presidential election and cooperation with the declassification process.

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 analyzing and countering these threats are neither sufficient nor closely coordinated. The Committee includes provisions within this legislation to address these concerns.

Framework for Cybersecurity and Intelligence Collection Doctrine

The Committee directs the ODNI, in coordination with appropriate IC elements, to develop an analytic framework that could support the eventual creation and execution of a government-wide cybersecurity and intelligence collection doctrine. The ODNI shall provide this framework, which may contain a classified annex, to the congressional intelligence committees, within 180 days of enactment of this Act.

This framework shall include:

1. An assessment of the current and medium-term cyber threats to the protection of the United States' national security systems and critical infrastructure;

2. Intelligence Community definitions of key cybersecurity concepts, to include cyberespionage, cyber theft, cyber acts of aggression, and cyber deterrence;

3. Intelligence collection requirements to ensure identification of cyber actors targeting U.S. national security interests,

and to inform policy responses to cyber attacks and computer network operations directed against the United States;

4. The Intelligence Community's methodology for assessing the impacts of cyber attacks and computer network operations incidents directed against the United States, taking into account differing levels of severity of incidents;

5. Capabilities that the IC could employ in response to cyber attacks and computer network operations incidents, taking into account differing levels of severity of incidents;

6. A policy and architecture for sharing cybersecurity-related intelligence with government, private sector, and international partners, including existing statutory and other authorities which may be exercised in pursuit of that goal; and

7. Any necessary changes in IC authorities, governance, technology, resources, and policy to provide more capable and agile cybersecurity.

Inspector General of the Intelligence Community Role and Responsibilities

The Inspector General of the Intelligence Community (IC IG) was codified by the *Intelligence Authorization Act for Fiscal Year 2010* to "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 IC's 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 the IC IG's role be 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 also 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 IG across the IC will fully cooperate with the direction provided elsewhere in the bill to ensure both the DNI 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 *Intelligence Authorization Act for Fiscal Year 2017,* 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 with how state investments in these spaceports may support infrastructure improvements, such as payload integration and launch capabilities, for national security launches.

Project MAVEN

Project MAVEN provides important capabilities for the acceleration of ongoing efforts to integrate big data, artificial intelligence, and machine learning, and ensure our warfighters maintain an advantage over our adversaries. Ensuring coordinated investment between the Department of Defense and the Intelligence Community is specifically critical for improving object detection, identification, and tracking of targets.

Therefore, the Committee directs the Secretary of Defense, in coordination with relevant IC elements, to brief the congressional intelligence and defense committees, within 90 days of enactment of this Act, on the following aspects of Project MAVEN: a strategy for coordinating and validating requirements; a methodology for cataloging data; development and deployment of algorithms; a technology investment plan; and a plan for fielding Project MAVEN capabilities.

Acquisition Research Center postings

The Committee supports a flexible National Reconnaissance Office (NRO) acquisition process that allows the NRO to choose the most appropriate contracting mechanism, whether for small research and development efforts or large acquisitions. The NRO's Acquisition Research Center (ARC), a classified contracting and solicitation marketplace that NRO and other agencies use, enables this flexible acquisition process for classified efforts.

The Committee directs the NRO, within 60 days of enactment of this Act, to brief the congressional intelligence and defense committees on options for modifying ARC posting procedures to ensure fair and open competition. Those options should include ensuring that unclassified NRO solicitations are posted on the unclassified FEDBIZOPS site, and identifying ways to better utilize the ARC to encourage contract opportunities for a more diverse industrial base that includes smaller and non-traditional companies.

Ensuring strong strategic analytical tradecraft

The DHS's Office of I&A has taken steps to improve the quality of its analysis, to identify its core customers, and to tailor its production to meet customer needs. The Committee concurs with I&A's implementation of analytic standards and review mechanisms that have improved the tradecraft behind I&A productions. The bedrock of these efforts has been the development of a yearly program of analysis (POA) and key intelligence questions, which are essential tools for providing a roadmap and boundaries for the office's production efforts.

Therefore, the Committee directs the Office of I&A to continue to prioritize, develop and hone its strategic intelligence capabilities and production, including the annual development of a POA. Within 90 days of enactment of the Act, and on an annual basis thereafter for two years, I&A shall brief the congressional intelligence committees on the development and execution of its POA. These

briefings should provide an overview of the POA, how customer needs have been incorporated into the POA, and an update on execution against the POA.

Cyber/Counterintelligence analysis

DHS's Office of I&A's Counterintelligence Mission Center analysis focuses on counterintelligence threats posed by foreign technology companies and fills a gap in IC intelligence production. Advanced technologies are increasingly ubiquitous and necessary to the function of modern society. Consequently, the scope of the threats from countries intent on using these technologies as a vector for collecting intelligence from within the United States will continue to expand. The Office of I&A is well positioned to conduct a niche analysis critical to national security that combines foreign intelligence with domestic threat information.

The committee strongly supports I&A's Counterintelligence Mission Center's continued focus on these topics and the increased resources the Fiscal Year 2019 dedicated to this analysis. Therefore, the Committee directs the Office of I&A, in coordination with ODNI, to provide an update within 90 days of enactment of this Act on its recent analytic production related to counterintelligence threats posed by foreign technology companies, including a review of the countries and companies that present the greatest risks in this regard.

Intelligence support to the export control process

The Committee has significant concerns that China poses a growing threat to United States national security, due in part to its relentless efforts to acquire United States technology. China purposely blurs the distinction between its military and civilian activities through its policy of "military-civilian fusion," which compounds the risks of diversion of United States technology to the Chinese military.

The Committee concludes that the United States Government currently lacks a comprehensive policy and the tools needed to address this problem. China exploits weaknesses in existing U.S. mechanisms that are aimed at preventing dangerous technology transfers, including the U.S. export control system, which is run by the U.S. Department of Commerce's Bureau of Industry and Security (BIS). The Committee has specific concerns about the lack of adequate and effective IC support to BIS's export license application review process and believes more robust IC support could have prevented many of the ill-advised technology transfers that have occurred in recent years.

Therefore, the Committee directs the DNI to submit a plan, within 120 days of enactment of this Act, to describe how the IC will provide BIS with, at a minimum, basic but timely analysis of any threat to U.S. national security posed by any proposed export, reexport, or transfer of export-controlled technology. The plan shall include detailed information on the appropriate organizational structure, including how many IC personnel would be required, where they would be located (including whether they would be embedded at BIS to coordinate IC support), and the amounts of necessary funding. In formulating the plan, the DNI should study the "National Security Threat Assessment" process that the National

Intelligence Council uses to inform the actions of the Committee on Foreign Investment in the United States. The DNI shall submit the plan to the congressional intelligence committees in classified form.

Social media

The Committee encourages the IC, notably the FBI, to both continue and enhance its efforts to assist in detecting, understanding, and warning about foreign influence operations using social media tools to target the United States. Additionally, within the scope of the IC's authorities, and with all necessary protections for U.S. person information, the Committee encourages the IC to augment and prioritize these ongoing efforts.

Trade-based money laundering

Threats to our national security posed by trade-based money laundering are concerning. Therefore, the Committee directs the DNI, within 90 days of enactment of this Act, to submit a report to the congressional intelligence committees on these threats, including an assessment of the severity of the threats posed to the United States' national security by trade-based money laundering conducted inside and outside the United States; an assessment of the scope of the financial threats to the U.S. economy and financial systems posed by trade-based money laundering; a description of how terrorist financing and drug trafficking organizations are advancing their illicit activities through the use of licit trade channels; an assessment of the adequacy of the systems and tools available to the Federal Government for combating trade-based money laundering; and a description and assessment of the current structure and coordination between Federal agencies, as well as with foreign governments, to combat trade-based money laundering. The report shall be submitted in classified form with an unclassified summary for public availability.

COMMITTEE ACTION

On June 26, 2018, 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 annexes for Fiscal Years 2018 and 2019, the base text for purposes of amendment.

By unanimous consent, the Committee agreed to amending the bill's title to be the *Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019.*

By voice vote, the Committee adopted en bloc nine amendments to the classified annex, as sponsored by: (1) Chairman Burr and Vice Chairman Warner; (2) Senator Rubio, and cosponsored by Senator Cornyn and Senator Manchin; (3) Senator Rubio, and cosponsored by Senator Heinrich; (4) Senator King, and cosponsored by Senator Cornyn; (5) Senator Cotton, and cosponsored by Senator Rubio, Senator Cornyn, and Senator Manchin; (6) Senator Manchin; (7) Senator Harris, and cosponsored by Senator Heinrich;

(8) Senator Harris; and (9) Chairman Burr and Vice Chairman Warner, as to overall funding adjustments.

By voice vote, the Committee adopted en bloc seven amendments to the bill: (1) an amendment by Vice Chairman Warner regarding information sharing for positions of trust; (2) an amendment by Senator Wyden, and cosponsored by Senator Rubio, Senator Heinrich, and Senator Harris, regarding state election officials' clearance eligibility; (3) an amendment by Senator Wyden, and cosponsored by Senator Heinrich, regarding cyber protection for certain IC personnel; (4) an amendment by Senator Wyden regarding protections for confidentiality of whistleblower-related communications; (5) an amendment by Senator Wyden regarding a study and report on the feasibility of encrypting unclassified wireline and wireless telephone calls; (6) an amendment by Senator Heinrich regarding the IC's procurement authority to protect against supply chain risks; and (7) an amendment by Senator Harris to expand and clarify IC reporting on diversity.

By voice vote, the Committee adopted a second-degree amendment by Chairman Burr to an amendment by Senator Cotton to the classified annex.

By voice vote, the Committee adopted the amendment by Senator Cotton to the classified annex, as modified by the second-degree amendment by Chairman Burr.

By a vote of 6 ayes to 9 noes, the Committee did not adopt an amendment by Senator Rubio, and cosponsored by Senator Feinstein and Senator Cornyn, regarding creditable service for federal retirement for certain individuals. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—aye; Senator Rubio—aye; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—aye; Senator Cornyn—aye; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—no; Senator Heinrich—no; Senator King—no; Senator Manchin—no; and Senator Harris—no.

By voice vote, the Committee did not adopt an amendment by Senator Lankford, regarding the Foreign Intelligence Surveillance Court.

By a vote of 14 ayes to 1 no, the Committee adopted a second-degree amendment by Senator King to an amendment by Senator Wyden that prohibits IC officers nominated to Senate-confirmed positions from making certain classification determinations, and would have required advisory opinions from the Public Interest Declassification Board. The second-degree amendment struck the Public Interest Declassified Board requirement. 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 a vote of 14 ayes to 1 no, the Committee adopted the amendment by Senator Wyden that prohibits IC officers nominated to Senate-confirmed positions from making certain classification determinations, as modified by the second-degree amendment by Senator King. 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—no; Senator Cornyn—aye; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Manchin—aye; and Senator Harris—aye.

By a vote of 6 ayes to 9 noes, the Committee did not adopt an amendment by Senator Wyden, and cosponsored by Senator Feinstein, Senator Heinrich, and Senator Harris, regarding IC reporting on IC resources used for certain travel and vetting initiatives. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Rubio—no; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Senator Cornyn—no; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Manchin—no; and Senator Harris—aye.

By a vote of 7 ayes to 8 noes, the Committee did not adopt an amendment by Senator Heinrich, regarding limitations on intelligence sharing with the Republic of Korea and the Democratic People's Republic of Korea. The votes in person or by proxy were as follows: Chairman Burr—no; Senator Risch—no; Senator Rubio—no; Senator Collins—no; Senator Blunt—no; Senator Lankford—no; Senator Cotton—no; Senator Cornyn—no; Vice Chairman Warner—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Heinrich—aye; Senator King—aye; Senator Manchin—aye; and Senator Harris—aye.

Senator Feinstein filed two amendments regarding the Foreign Agents Registration Act that she did not offer.

Senator Wyden filed three amendments regarding the appointment of an Executive Director for IC whistleblowing and source protection, striking the Sense of Congress on WikiLeaks, and modifying unauthorized disclosures reporting, respectively, that he did not offer.

Vote to report the committee bill

The Committee voted to report the bill unanimously, as amended, by a vote of 15 ayes and zero noes. 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—aye; 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 au-

thorizations. 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 28, 2018, 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 SENATORS WYDEN, HEINRICH, AND HARRIS

We have sought information from the DNI on whether and to what extent Intelligence Community resources are intended to support the implementation of travel and vetting-related Executive Orders, ICE's "Extreme Vetting Initiative," and any expansion of vetting of DACA recipients, people granted temporary protected status, or the general undocumented immigrant population. We are working with Committee leadership in obtaining this information in a timely manner.

ADDITIONAL VIEWS OF SENATOR WYDEN

The Fiscal Year 2019 Intelligence Authorization bill includes eight important amendments I offered, three of which carried over from the Fiscal Year 2018 bill.

The first amendment requires reporting from the Director of National Intelligence, in coordination with the Department of the Treasury, 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 reporting 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 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 carried over from the Fiscal Year 2018 bill 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 2017 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.

The Fiscal Year 2019 bill includes five new amendments I offered. The first requires a report from the DNI, in coordination with the Inspector General of the Intelligence Community, on the protection of whistleblower-related communications in the context of "continuous evaluation" of persons with security clearances. "Continuous evaluation," in particular monitoring of communica-

tions, risks violating the confidentiality of whistleblowers and chilling whistleblower activities. Such a result would not only deprive the government of knowledge of waste, fraud and abuse, but could lead to more unauthorized disclosures, the very problem the continuous evaluation policy is intended to address.

I offered two amendments that will help protect the unclassified communications of Intelligence Community personnel. The first, cosponsored by Senator Heinrich, permits the DNI to provide cyber protection support for the personal devices and accounts of Intelligence Community personnel who are especially vulnerable to cyber attacks and hostile collection activities. The second amendment requires the DNI to conduct a study on the feasibility of encrypting unclassified communications among Intelligence Community personnel. Intelligence Community personnel should never communicate classified information through unclassified channels and should limit business to official devices and accounts. Nonetheless, these amendments recognize the reality that unclassified and personal communications may be of significant interest to our adversaries and should thus be secured to the greatest extent possible.

The bill includes an amendment I offered with Senators Rubio, Heinrich, and Harris that removed the underlying bill's limits on the number of state election officials granted security clearances. As states and localities work to combat the evolving cyber threat to our election infrastructure, they will need additional assistance from the federal government, including the provision of classified threat information. It is thus critical that the Department of Homeland Security and the states have flexibility in ensuring that the people who need the information to safeguard our elections receive it.

Finally, the bill includes an amendment I offered with Senators King, Heinrich, and Harris that prohibits Intelligence Community officers who are nominated to Senate-confirmed positions from making classification decisions about themselves. The amendment addresses a clear conflict of interest problem in which the officer could engage in selective classification and declassification in a manner that helps him or her get confirmed. The amendment gives the decision to the DNI, or the Principal Deputy DNI should the nominated officer be the DNI him or herself. It also requires a report to the congressional intelligence committees on the reasons for the decision. The amendment originally required an advisory opinion from the Public Interest Declassification Board (PIDB), which would have added an independent perspective to the process. While I am disappointed that this requirement was removed, the amendment is nonetheless an important step forward.

I remain concerned with a provision in the bill, carried over from Fiscal Year 2018, stating that it is the Sense of Congress "that WikiLeaks and the senior leadership of WikiLeaks resemble a nonstate 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, constitu-

tional, and policy implications, particularly should it be applied to journalists inquiring about secrets.

CHANGES TO EXISTING LAW

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

○