AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 244

113TH CONGRESS *1st Session* | SENATE | REPORT 113–120

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2014

NOVEMBER 13, 2013.—Ordered to be printed

Mrs. FEINSTEIN, from the Select Committee on Intelligence, submitted the following

R E P O R T

[To accompany S. 1681]

The Select Committee on Intelligence, having considered an original bill (S. 1681) to authorize appropriations for fiscal year 2014 for intelligence and intelligence-related activities of the United States Government and the Office of the Director of National Intelligence, 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 27, 2013, 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 (NIP) for Fiscal Year 2014 is $52.2 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 Act and has the legal status of public law. The classified annex is made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President. It is also available for review by any Member of

the Senate subject to the provisions of Senate Resolution 400 of the 94th Congress (1976).

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the Intelligence Authorization Act for Fiscal Year 2014 that is being reported by the Committee.

TITLE I—BUDGET AND PERSONNEL AUTHORIZATIONS

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 2014.

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 and the applicable personnel levels by program for Fiscal Year 2014 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 is intended to provide additional flexibility to the DNI in managing the civilian personnel of the Intelligence Community (IC). Section 103(a) provides that the DNI may authorize employment of civilian personnel in Fiscal Year 2014 in excess of the number of authorized positions by an amount not exceeding three percent of the total limit applicable to each IC element under Section 102. The DNI may do so only if necessary to the performance of important intelligence functions.

Section 103(b) requires the DNI to establish guidelines that would ensure a uniform and accurate method of counting certain personnel under a system of personnel levels. The DNI has issued such a policy. Subsection (b) confirms in statute the obligation of the DNI to establish these guidelines.

Section 103(c) provides that the DNI must report the decision to allow an IC element to exceed the personnel ceiling in advance to the congressional intelligence committees.

Section 104. Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the DNI and sets the authorized personnel levels for the elements within the ICMA for Fiscal Year 2014.

Subsection (a) authorizes appropriations of $568,736,000 for Fiscal Year 2014 for the activities of the ICMA. Subsection (b) authorizes 855 positions for elements within the ICMA for Fiscal Year 2014 and provides that such personnel may be permanent employees of the Office of the Director of National Intelligence (ODNI) or detailed from other elements of the United States Government.

Subsection (c) authorizes additional appropriations and positions for the classified Community Management Account as specified in the classified Schedule of Authorizations and permits the funding for advanced research and development to remain available through September 30, 2015.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $514,000,000 for Fiscal Year 2014 for the Central Intelligence Agency (CIA) Retirement and Disability Fund.

Section 202. CIARDS and FERS special retirement credit for service on detail to another agency

Section 202 amends the Central Intelligence Agency Retirement Act to clarify that "qualifying service" for purposes of obtaining certain enhanced retirement benefits available to CIA employees who carry out duties abroad that are hazardous to life or health or involve specialized skills includes service while on detail to another government agency.

CIA recently informed the Committee that a number of Agency employees on detail to other intelligence agencies who otherwise qualify for enhanced retirement benefits, and had been advised by prior CIA leadership that they were entitled to those additional benefits, would be denied the enhanced benefits because the Central Intelligence Agency Retirement Act does not extend such benefits to CIA employees on detail to another intelligence agency. Section 202 corrects this inequity by clarifying that "qualifying service" includes service on detail to another agency.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

SUBTITLE A—GENERAL 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 this 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. OPEN FOIA protections

Section 303 amends Section 103H of the National Security Act, the organic statute for the Inspector General of the Intelligence Community, to provide that the identity of an individual who makes a complaint or provides information may be withheld in response to a request under the Freedom of Information Act (FOIA).

Under FOIA, information may be withheld in response to a FOIA request pursuant to a statute that requires that matters be withheld from the public in such a manner as to leave no discretion, or establishes criteria for withholding information or referring to particular types of matters to be withheld and specifically cites to FOIA. The OPEN FOIA Act of 2009 (PL 111–83, sec. 564, October 28, 2009) requires that a statute providing an exemption from disclosure under FOIA, if enacted after the date of enactment of the OPEN FOIA Act of 2009, must specifically cite Section 552(b)(3) of Title 5, United States Code. The organic statute for the Inspector General of the Intelligence Community (PL 111–259, sec. 405) was enacted at a later date, October 7, 2010. Accordingly, while Title 5 Inspectors General may exercise this authority without a reference to Section 552(b)(3), the OPEN FOIA Act requires that the Inspector General of the Intelligence Community's statute have a specific reference to Section 552(b)(3), as amended by the OPEN FOIA Act, to be operative. Section 303 provides the necessary reference.

Section 304. Functional managers

Section 304(a) codifies in statute the existing requirement, under Section 1.3 of Executive order 12333, to designate functional managers for signals intelligence (SIGINT), human intelligence (HUMINT), and geospatial intelligence (GEOINT), and other intelligence disciplines. At present, the functional managers for SIGINT, HUMINT, and GEOINT are the Director of the National Security Agency (NSA), the Director of the CIA, and the Director of the National Geospatial-Intelligence Agency (NGA), respectively. In addition, Section 304(a) gives responsibility for designating functional managers to the President. Under Executive order 12333, the functional managers are designated by the DNI.

Section 304(b) codifies the existing responsibilities of the functional managers to act as the principal adviser to the DNI for their respective intelligence function. Section 304(b) also specifies that the functional managers shall act in the same capacity for the Secretary of Defense.

Section 304(c) establishes a new requirement for each functional manager to report to Congress annually on the state of their function, scheduled to occur no later than two weeks after the President's budget submission. The reporting requirement calls on each functional manager to identify those programs, projects, and activities that comprise the intelligence discipline for which they are responsible (regardless of the funding source) and to report on resource issues and other matters relevant to the state of the function.

Section 305. Auditability

Section 305 requires the ODNI, CIA, Defense Intelligence Agency (DIA), NGA, National Reconnaissance Office (NRO), and NSA to undergo full financial audits conducted by internal or external independent accounting or auditing organizations beginning with each agency's Fiscal Year 2014 financial statements. In addition, each of the aforementioned agencies is required to obtain an unqualified opinion not later than the audit of their Fiscal Year 2016 financial statements. The chief financial executive of each of the

aforementioned agencies is required to provide to the congressional intelligence committees an annual report of each audit conducted.

Section 306. Software licensing

Section 305 of the Intelligence Authorization Act for Fiscal Year 2013 required the chief information officers of each element of the IC to conduct an inventory of software licenses held by such element, including both utilized and unutilized licenses. Section 305 also required that the Chief Information Officer of the Intelligence Community (CIO) report those inventories to the congressional intelligence committees within 180 days of enactment of the Fiscal Year 2013 Act. The Committee received that report on August 22, 2013.

Section 306(a) builds upon Section 305 of the Fiscal Year 2013 Act by requiring that every two years the chief information officers of each element of the IC: (1) conduct an inventory of software licenses held by such element, including both utilized and unutilized licenses held by the element, and (2) assess the actions that could be carried out by such element to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage. Section 306(a) also specifies that the initial inventories and assessments shall be based on the inventories that were required under Section 305 of the Fiscal Year 2013 Act.

Section 306(b) provides that, not later than 180 days after enactment, and every two years thereafter, the CIO shall compile an inventory of all existing software licenses of the IC and assess actions that could be carried out by the IC to achieve the greatest possible economies of scale and associated cost savings in software procurement and usage.

Section 306(c) requires that the CIO submit to the congressional intelligence committees a copy of each inventory compiled under Section 306(b).

Section 307. Public Interest Declassification Board

Section 307 extends the current authorization for the Public Interest Declassification Board (PIDB) from December 31, 2014 until December 31, 2018. The PIDB was created in the Intelligence Authorization Act for Fiscal Year 2000 to promote public access to a thorough, accurate, and reliable documentary record of significant United States national security decisions and activities.

Section 308. Reports of fraud, waste, and abuse

Section 308 amends Section 8H of the Inspector General Act of 1978, as amended, to expressly permit IC employees and contractors who intend to report a complaint or information with respect to an urgent concern to Congress to first report those complaints or urgent concerns to their respective agency Inspector General as well as the Inspector General of the Intelligence Community.

SUBTITLE B—TARGETED LETHAL FORCE OVERSIGHT

Section 311. Targeted lethal force oversight reform

Section 311 requires that the head of an element of the IC notify the DNI upon a determination that a particular, known United States person is knowingly engaged in acts of international ter-

rorism against the United States, such that the United States Government is considering the legality or the use of targeted lethal force against that United States person. Not later than 15 days after the date the DNI receives such a notification from the head of an element, the DNI is required to complete an independent alternative analysis of the determination made by the head of the notifying element. In addition, the DNI is required to report, as soon as practicable, to the Inspector General of the Intelligence Community and the congressional intelligence committees.

Section 311 also requires that the Inspector General of the Intelligence Community conduct an annual review of IC compliance with all appropriate policies and procedures related to consideration of the use of targeted lethal force against particular, known United States persons and to report the findings to the DNI and the congressional intelligence committees.

Section 311 does not prohibit a department or agency of the United States Government from using targeted lethal force against a United States person pending notification of the DNI or completion of the independent alternative analysis. This section is intended to require independent alternative analysis of the analytic judgments made by IC elements in support of a determination to use targeted lethal force against a United States person. It is not intended to require independent alternative analysis of the determination to use such force or the legality of such use by a department or agency of the United States Government.

Section 312. Unclassified annual report on the use of targeted lethal force outside the United States

Section 312 requires that the President prepare and make public an annual report that sets forth the total number of combatants and noncombatant civilians killed or injured during the preceding year by the use of targeted lethal force outside the United States by remotely piloted aircraft. The reporting requirement under this section does not apply to any use of targeted lethal force in Afghanistan prior to the end of combat operations by the United States or to any use of targeted lethal force pursuant to a declaration of war or authorization for the use of military force, where such declaration or authorization is issued after the date of enactment of this section. This section requires the President to make public aggregate annual figures for combatants and noncombatant civilians killed or injured by the use of targeted lethal force, regardless of whether such deaths or injuries are intended or unintended. It does not require the President to report specific information concerning individual uses of force or the entity responsible for such uses.

SUBTITLE C—REPORTING

Section 321. Opinions of the Office of Legal Counsel concerning intelligence activities

Section 321(a) requires that the Attorney General provide the congressional intelligence committees a listing of every opinion of the Office of Legal Counsel (OLC) of the Department of Justice that has been provided to an element of the IC, whether classified or unclassified.

Section 321(b) provides an exception to the listing requirement in Section 321(a) when the President determines that it is essential to limit access to a covert action finding under Section 503(c)(2) of the National Security Act. In such cases, the President may limit access to information concerning such a finding that is subject to disclosure under Subsection (a) to those members of Congress who have been granted access to the relevant finding.

Section 321(c) provides a second exception to the disclosure requirements in Section 321(a) where the President determines that information subject to disclosure under Subsection (a) is subject to Executive privilege. In such cases, the Attorney General must notify the congressional intelligence committees, in writing, of the legal justification for the assertion of the privilege prior to the date by which the opinion or listing is required to be disclosed.

The Committee regularly conducts oversight of intelligence activities that are the subject of one or more OLC legal opinions. These opinions often represent the best and most comprehensive expression of the legal basis for the intelligence activities that the Committee oversees. The Committee regards access to these legal opinions as necessary to the performance of its oversight functions and often requests access to such opinions, or the legal analysis contained in such opinions, when the Committee is made aware of their existence.

While the Committee generally is kept apprised of the legal basis for U.S. intelligence activities, as required by Sections 502 and 503 of the National Security Act of 1947, neither the Department nor the IC routinely advises the Committee of the existence of OLC opinions that are relevant to the Committee's oversight functions. This presents an impediment to the Committee's oversight function, as the Committee cannot request access to legal analysis when it is not made aware that such analysis exists. Section 321 would ensure that the Committee is aware of the existence of relevant OLC opinions so that it can obtain access to the legal analysis set forth in these opinions through a process of accommodation with the Executive branch.

The Committee recognizes that, in certain limited cases, the fact that an OLC opinion exists may be entitled to Executive privilege or may reveal information concerning certain compartmented covert action programs. Therefore, Subsections 321(b) and (c) provide exceptions for such cases.

Section 322. Submittal to Congress by heads of elements of intelligence community of plans for orderly shutdown in event of absence of appropriations

Section 322 requires the head of each element of the IC, upon submission of a plan pertaining to agency operations in the absence of appropriations to the Director of the Office of Management and Budget, to submit a copy of such plan to the congressional committees of jurisdiction in a manner consistent with security handling requirements. During the most recent government shutdown, such plans pertaining to elements of the IC were neither publicly available because of classification constraints, nor readily provided to the Committee.

Section 323. Reports on chemical weapons in Syria

Section 323 directs the DNI to submit to the appropriate congressional committees, within 30 days, a report on the Syrian chemical weapons program containing specific elements as described in Subsection 323(b). In addition, Section 323 requires the DNI to provide the appropriate congressional committees with progress reports every 90 days that include any material updates on the Syrian chemical weapons program.

Section 324. Reports to the Intelligence Community on penetrations of networks and information systems of certain contractors

Section 324 directs the DNI to establish procedures that require cleared intelligence contractors to notify the government of any successful unauthorized penetration of the contractor's network or information systems and to provide the government with access to such systems in order to perform forensic analysis in the event of such a penetration.

Section 325. Repeal or modification of certain reporting requirements

Congress frequently requests information from the IC in the form of reports, the contents of which are specifically defined by statute. The reports prepared pursuant to these statutory requirements provide Congress with an invaluable source of information about specific matters of concern.

The Committee recognizes, however, that congressional reporting requirements, and particularly recurring reporting requirements, can place a significant burden on the resources of the IC. The Committee reconsiders these reporting requirements on a periodic basis to ensure that the reports that have been requested are the best mechanism for the Congress to receive the information it seeks. In some cases, annual reports can be replaced with briefings or notifications that provide the Congress with more timely information and offer the IC a direct line of communication to respond to congressional concerns.

In response to a request from the DNI, the Committee examined a set of recurring reporting requirements nominated by the IC, including those which arise from legislation reported or managed by committees other than the congressional intelligence committees. Section 325 eliminates three reports that were burdensome to the IC when the information in the reports could be obtained through other means or was no longer considered relevant to current concerns. Section 325 also modifies four reports to replace requirements for annual reports with notification requirements, sunsets a report one year earlier, and changes the periodicity of a report from a quarterly basis to a semiannual basis.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—NATIONAL SECURITY AGENCY

Section 401. Appointment of the Director of the National Security Agency

Section 401 amends the National Security Agency Act of 1959 to provide that the Director of the NSA shall be appointed by the President by and with the advice and consent of the Senate. Under present law and practice, the President appoints the Director of the NSA. The appointment has been indirectly subject to confirmation through Senate confirmation of the military officers who have been promoted into the position. Section 401 will make explicit that the filling of this key position in the Intelligence Community should be subject to Senate confirmation.

The Committee has had a long-standing interest in ensuring Senate confirmation of the Director of the NSA, and this requirement has previously been supported by the Senate. The Committee renews the requirement for Senate confirmation of the Director of NSA in this Act in light of NSA's critical role in the national intelligence mission, particularly with respect to activities that may raise privacy concerns.

Through advice and consent, the Senate can enable the Congress to fulfill more completely its responsibility for providing oversight of the intelligence activities of the United States Government and ensure that the NSA's responsibilities and foreign intelligence activities receive appropriate attention.

Section 401 does not alter the role of the Committee on Armed Services of the Senate in reviewing and approving the promotion or assignment of military officers. The Committee intends to approve a separate Senate Resolution that would dictate the roles of the Committee and the Armed Services Committee in considering the nomination of a new Director of the NSA, with the order of the committees' actions to be determined by whether the nominee is a military officer.

Finally, the section makes clear that the requirement for Senate confirmation applies prospectively. Therefore, the Director of the NSA on the date of enactment will not be affected by this section, which will apply initially to the appointment and confirmation of his successor.

Section 402. Appointment of the Inspector General of the National Security Agency

Section 402 amends the Inspector General Act of 1978 (5 U.S.C. App.) to provide that the Inspector General of the NSA shall be appointed by the President by and with the advice and consent of the Senate. Under present law and practice, the Director of the NSA appoints the NSA Inspector General.

The Inspector General of the NSA performs a critical role in ensuring that the NSA carries out its national intelligence mission in full compliance with the law and applicable policies and regulations. By requiring Presidential appointment and Senate confirmation of the NSA Inspector General, this provision will ensure the NSA Inspector General operates independently of the Director of

the Agency in overseeing the activities of the NSA, particularly with respect to activities that may raise privacy concerns.

SUBTITLE B—NATIONAL RECONNAISSANCE OFFICE

Section 411. Appointment of the Director of the National Reconnaissance Office

Section 411 amends the National Security Act of 1947 (50 U.S.C. 3001 et seq.) to provide that the Director of the NRO shall be appointed by the President by and with the advice and consent of the Senate.

The Director of the NRO is responsible for a number of highly technical programs that involve the obligation and expenditure of significant sums of appropriated funds. By requiring Presidential appointment and Senate confirmation of the NRO Director, Congress will be better able to fulfill its responsibility for providing oversight of these important programs.

Section 412. Appointment of the Inspector General of the National Reconnaissance Office

Section 412 amends the Inspector General Act of 1978 (5 U.S.C. App.) to provide that the Inspector General of the NRO shall be appointed by the President by and with the advice and consent of the Senate. Under present law and practice, the Director of the NRO appoints the NRO Inspector General.

The Inspector General of the NRO performs a critical role in overseeing complex, high-dollar value programs conducted by the NRO. In the past, the NRO Inspector General has been successful in identifying significant instances of fraud, waste, and abuse within the NRO. By requiring Presidential appointment and Senate confirmation of the NRO Inspector General, this provision will ensure the NRO Inspector General continues to operate with appropriate independence from the NRO Director in overseeing the activities of the NRO.

TITLE V—SECURITY CLEARANCE REFORM

Section 501. Appropriate committees of Congress defined

Section 501 defines the term "appropriate committees of Congress" for this title.

Section 502. Technology improvements to security clearance processing

Section 502 requires the DNI, in consultation with the Secretary of Defense and the Director of the Office of Personnel Management (OPM), to conduct an analysis of the relative costs and benefits of potential improvements to the process for investigating persons who are proposed for access to classified information and adjudicating whether such persons satisfy the criteria for obtaining and retaining access to such information.

Section 503. Enhanced reciprocity of security clearances

Section 503 amends Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(d)) to include a provision that prohibits an agency from rejecting another agency's determination that an individual is eligible for access to classified

information on the basis that such eligibility determination is out-of-scope, unless the rejecting agency certifies that it does not employ any personnel who have background investigations that also are out-of-scope.

Section 503 also amends Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 3341(d)) to establish a presumption that personnel who have been determined to be eligible for access to classified information also are suitable for employment.

The Committee understands that some agencies have denied security clearance reciprocity for some IC personnel where an eligibility determination is out-of-scope, even when the agency employs personnel whose eligibility determinations also are out of scope. In addition, the Committee understands that some agencies have delayed employment of personnel who have been determined to be eligible for access to classified information while the agency adjudicates their suitability for employment. The Committee believes that both of these practices inappropriately impede the movement of cleared personnel between agencies, often at significant cost to the government.

Section 504. Report on reciprocity of security clearances

Section 504 requires the DNI to submit a report to Congress each year, through 2017, that provides information on the reciprocal treatment of security clearances, including (1) the periods of time required by authorized adjudicative agencies for accepting background investigations and determinations completed by an authorized investigative entity or authorized adjudicative agency, (2) the total number of cases in which a background investigation or determination completed by an authorized investigative entity or authorized adjudicative agency is accepted by another agency, and (3) the total number of cases in which a background investigation or determination completed by an authorized investigative entity or authorized adjudicative agency is not accepted by another agency.

Section 505. Improving the periodic reinvestigation process

Section 505 requires the DNI, in consultation with the Secretary of Defense and the Director of OPM to transmit to Congress each year, through 2017, a strategic plan for improving the process for periodic reinvestigations.

TITLE VI—INTELLIGENCE COMMUNITY WHISTLEBLOWER PROTECTIONS

Section 601. Protection of Intelligence Community whistleblowers

Section 601 would create a new Section 2303A of Title 5 of the United States Code, modeled on protections for Federal Bureau of Investigation (FBI) employees in Section 2303 of Title 5. This new section would prohibit taking a personnel action against an IC employee as a reprisal for making a protected whistleblower disclosure to the DNI (or his designee), the Inspector General of the Intelligence Community, the head of the employing agency (or his designee), the appropriate Inspector General of the employing agency, a congressional intelligence committee, or a member of a congressional intelligence committee. The President would be di-

rected to provide for enforcement of this section. The section also clarifies that this bill in no way affects the FBI provisions under Section 2303 of Title 5.

Section 602. Review of security clearance or access determinations

Section 602 would prohibit making security clearance and access determinations because of a protected whistleblower disclosure.

The section would direct the DNI to create procedures to allow appeals of adverse security clearance and access determinations alleged to be in retaliation for a protected disclosure. This section would create certain due process protections, including the right to an independent and impartial fact-finder; for notice and the opportunity to be heard, including the opportunity to present relevant evidence, including witness testimony; to be represented by counsel; to receive a decision based on the record developed; and to receive a decision within 180 days, unless the employee and the agency agree to an extension, or the impartial fact-finder determines in writing that a greater time period is needed in the interest of fairness or national security.

If whistleblower retaliation is found, the agency would be required to take corrective action, which could include back pay, costs, and compensatory damages not to exceed $300,000. Relief may not be granted if the agency demonstrates by a preponderance of the evidence that it would have taken the same personnel action absent the disclosure, giving the utmost deference to the agency's assessment of the particular threat to United States national security interests.

Classified information may be used in the process, including through ex parte submissions if the agency determines that national security interests so warrant. The employee would have no right to compel the production of classified information except as necessary to establish that the employee made a protected disclosure. The DNI would be directed to create procedures to allow individuals to retain government employment, to the extent practicable, during this appeal process. However, an appeal of an agency's suspension of a security clearance or access determination for the purposes of conducting an investigation would not be allowed if a suspension lasts longer than one year.

An employee would be permitted to appeal the agency's decision within 60 days of receiving it. The appellate board's review would be de novo, based on the complete agency record and any portions of the record that were submitted ex parte shall remain ex parte during the appeal. If the board determines that further fact-finding is necessary, it would remand the matter to the agency for additional proceedings. If the board finds that an adverse security clearance or access determination violated this section, it would order corrective action. The board would then separately determine whether reinstituting the security clearance or access determination is clearly consistent with national security, with any doubt resolved in favor of national security. The board may recommend, but may not order, reinstatement of the security clearance or access determination. Additionally, the board may recommend, but not order, reinstatement or the rehiring of a former employee. The board may order that the former employee be treated as though the employee were transferring from the most recent position held

when seeking other federal employment. The agency would be required to take the actions ordered within 90 days, unless the DNI, Secretary of Defense, or Secretary of Energy determines that doing so would endanger national security. Congressional notification of board orders would be required, but neither judicial review nor a private cause of action would be permitted.

Section 603. Revisions of other laws

Section 603 amends the Inspector General Act of 1978 and the Central Intelligence Agency Act of 1949 to establish procedures for resolving instances in which a complaint or information would create a conflict of interest. In addition, Section 603 amends the Inspector General Act of 1978, the Central Intelligence Agency Act of 1949, and the National Security Act of 1947 to authorize an individual who has submitted a complaint or information to an Inspector General under those acts to notify any member of Congress or congressional staff member of the fact that such individual has made such submission.

Section 604. Regulations; reporting requirements; nonapplicability to certain terminations

Section 604 would require the DNI to issue regulations to carry out the IC protections created by Section 601 and to report to Congress on the implementation of these regulations within two years. This section also would require the DNI to establish the appellate board referenced in Section 602.

Section 604 also provides that the legislation affords no protections for certain terminations of employment: (1) those under 10 U.S.C. 1609; and (2) those personally and summarily carried out by the DNI, the Director of the CIA, or an agency head under 5 U.S.C. 7532, if the Director or agency head determines the termination to be in the interest of the United States, determines that the procedures prescribed in other provisions of law that authorize the termination of the employee's employment cannot be invoked in a manner consistent with national security, and notifies Congress within five days of the termination.

TITLE VII—OTHER MATTERS

Section 701. Repeal of the termination of notification requirements regarding the authorized disclosure of national intelligence

Section 701 eliminates the sunset for Section 504 of the Intelligence Authorization Act for Fiscal Year 2013. Section 504 of that Act requires government officials responsible for making certain authorized disclosures of national intelligence or intelligence related to national security to notify the congressional intelligence committees concurrent with such disclosures.

Section 702. Gifts, devises, and bequests

Section 702 amends Section 12 of the Central Intelligence Agency Act of 1949 in order to provide the Director of the CIA with express authority to engage in fundraising in an official capacity for the benefit of nonprofit organizations that provide support to surviving family members of deceased Agency employees or that otherwise provide support for the welfare, education, or recreation of Agency

employees, former Agency employees, or their family members. Section 702 limits such fundraising to active participation in the promotion, production, or presentation of an event designed to raise funds and requires that such fundraising adhere to ethical constraints established by the Office of Government Ethics.

Section 703. Budgetary effects

Section 603 provides that the budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go-Act of 2010, shall be determined by reference to the latest statement titled, "Budgetary Effects of PAYGO Legislation" for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

COMMITTEE COMMENTS

Analytic integrity

Since at least 2008, the IC has provided draft assessments for comment to policymakers and warfighters who have direct and potentially conflicting interests in the subjects being assessed. For example, commanders are asked to comment on IC assessments of aspects of their military missions and Ambassadors are asked to comment on IC analyses of trends in security or national politics within their country of assignment. In both examples, policymakers and warfighters have insights and access to unique information that should be reported and included as intelligence that informs the analytic debate. In each example, however, analysts are required to make assessments about issues that could reflect directly on the offices and operations of those asked to comment. This creates professional tension between the IC and policy communities and could put undue pressure on analysts to conform to the analysis provided by the more senior warfighter or policymaker.

Sound intelligence analysis requires that analysts who are dealing with issues of concern network in the United States and internationally to develop trusted relationships with partners external to the IC. These trusted relationships could include, as appropriate, experts in academia; think tanks; industry; nongovernmental organizations; the scientific world (e.g., U.S. Government laboratories, national academies, national research councils, and Federally Funded Research and Development Centers); state, local, tribal and territorial governments; and other non-IC U.S. Government agencies. These communities allow the IC to expand its knowledge base, share burdens, challenge assumptions and cultural biases, and encourage innovative thinking.

Such trusted relationships should be a key component of the normal integration, evaluation, and analysis of intelligence information that results in the production of finished intelligence judgments and assessments. Elements of the IC should use outside experts to closely review analytical assumptions, logic and, where appropriate, evidence, both during analysis and after assessments have been completed.

At the same time, the IC is responsible for ensuring that all finished intelligence is timely, objective, based on all available sources of information, independent of political consideration, and employs

the standards of proper analytic tradecraft. In view of this, no intelligence product of the IC should be unduly delayed or inappropriately altered to conform to the timelines or viewpoints of external partners, and care should be taken to avoid operational or policy-related conflicts of interest when seeking outside commentary. For example, IC assessments about the efficacy of a particular policy or covert action under consideration should not be altered to conform to the views of the policymakers crafting the policy. Likewise, assessments of the capabilities of foreign security services trained by the U.S. military or U.S.-led coalitions should not be delayed or altered to conform to the assessments of those responsible for the training.

Threat finance intelligence

Counter threat finance (CTF) leverages the capabilities of the interagency to help detect, deter, disrupt, and destroy terrorist organizations and those supporting terrorism by targeting the foundation of their operations, their financial resources. CTF is dependent upon the effective collection, analysis, and integration of Threat Finance Intelligence (TFI). TFI-enabled CTF is a critical component of the United States Strategy to Combat Transnational Organized Crime, which was released on July 25, 2011. A number of agencies within the IC have played a significant role in interagency CTF efforts against al-Qa'ida, the Taliban, and other key actors. IC agencies continue to develop and expand their ability to support efforts to disrupt our adversaries using the CTF discipline. IC support to the Iraq Threat Finance Cell (ITFC) under joint DOD-Department of Treasury leadership and the Afghan Threat Finance Cell (ATFC) under Drug Enforcement Agency leadership enabled efforts to identify and disrupt funding sources supporting insurgent and terrorist organizations, aided in the identification of key insurgency members and enablers, and supported TFI collection and analysis. It is important for the IC to ensure that lessons learned from these initiatives are captured and institutionalized to build upon successes and mature the IC's capability to apply the CTF discipline to new problem sets.

The Committee believes that the CTF discipline is an essential tool in combating transnational criminal networks and terrorist organizations worldwide, and believes it should be fully integrated into IC tradecraft, programmatic priorities, and operational planning. Furthermore, the IC must be able to integrate with, support, and enable other law enforcement and government agencies' CTF and TFI activities. Finally, it is important that the IC execute and organize TFI and CTF efforts throughout the community in a way that maximizes effectiveness and prevents duplication.

The Committee directs the DNI to submit to the congressional intelligence committees, not later than 180 days after enactment of this Act, a report outlining each CTF and TFI activity currently being planned or conducted by an element of the IC. Each summary should include a detailed description of the activity, identification of lead and supporting agencies, a description of each agency's role, the level and source of funding associated with each activity, a description of the desired outcomes from each activity, and a description of how this activity aligns with the goals of existing interagency strategies to address terrorism, corruption, crimes,

narcotics, and other transnational threats, including the United States Strategy to Combat Transnational Organized Crime. The report should also include a summary of operational lessons, best practices, and tools employed in ITFC and ATFC efforts, and how they can be replicated to advance other IC CTF missions. It should also include a description of the efforts, both within the IC and between the IC and other relevant agencies, to foster communication and ensure integrated support to interagency partners. Further, the report should identify any current gaps in the IC's CTF capabilities and authorities.

Suspension and debarment

The Committee is concerned that the IC does not have an IC-wide mechanism for identifying and tracking exploitative, unscrupulous, suspended or debarred contractors to ensure the Community deals only with vendors who are responsible in fulfilling their legal and contractual obligations. It is through the sharing of such information that the IC can make informed decisions, ensure the Community conducts business only with responsible contractors, prevent suspended and debarred contractors from initiating or repeating business throughout the IC, and avoid misuse or loss of potentially billions of dollars of taxpayer money.

Therefore, the Committee directs the DNI to develop a plan to meet the requirement, per the Federal Acquisition Regulation, to determine whether prospective vendors are debarred, suspended or listed on the federal government's System for Awards Management (SAM), a Web-based system maintained by the General Services Administration (GSA). Additionally, the DNI shall create an IC-wide Contractor Responsibility Watch List. This plan will be approved by the head of each IC element and the DNI, submitted to the congressional intelligence committees within 120 days of enactment of this bill, and implemented within a year of the date of such enactment.

DIA and NRO Financial Management System Study

The Committee has learned that implementation of the NSA's financial management system has experienced multiple delays and that the system requirements have been re-baselined since program inception. These delays have introduced additional risk for both the NSA and DIA towards achieving unqualified opinions on the Fiscal Year 2016 financial statements, as required by this Act. Therefore, the Committee requests that the DIA and the NRO conduct a joint study to determine the cost and feasibility of the DIA adopting the NRO's business systems and processes to the greatest extent possible. Additionally, the Committee requests that the NSA and the NRO conduct a joint study to determine the cost and feasibility of the NSA adopting the NRO's business systems and processes to the greatest extent possible.

The NGA and the NRO previously conducted a similar study. This study would serve as a useful basis for both of these new studies. The Committee requests that the joint study teams evaluate the cost, schedule, and performance requirements associated with implementing a system at both the DIA and the NSA, similar to that already in use at the NRO and the NGA.

The Committee requests that the chief financial executives of the DIA and the NSA, in association with the NRO, each complete a report and provide those reports to the congressional intelligence committees in 60 days.

Insider threats

The recent unauthorized disclosures to the media, and potentially to foreign adversaries, by Edward Snowden, a core contractor working at the National Security Agency, highlights the threat posed by insiders entrusted with access to IC facilities and networks.

The IC relies on a varied workforce comprised of civilians, uniformed military and core contractors to perform its work. These individuals are deployed at many government and contractor sites around the world. The IC also grants limited access to foreign partners, officials at the federal, state and local levels of government, and select representatives from industry. In this complex environment, the IC employs multi-layered counterintelligence and security measures to mitigate the potential threat posed by a trusted insider. It screens individuals through hiring, security clearance and contracting processes. The IC induces compliance through nondisclosure and secrecy agreements. It monitors these people over time through periodic reinvestigations, and financial and other regular reporting requirements. The IC monitors and audits behavior on official networks to detect inappropriate access and transmission of classified and sensitive information. The Justice Department punishes violations as a deterrent.

Despite this layered defense, there are still counterintelligence and security lapses. Mr. Snowden's decision to provide classified and sensitive information to the media will have ramifications for our national security for years to come. Initiatives have been underway for years to deal with such contingencies, most recently the President's National Insider Threat Policy, signed in November 2012. However, the Committee is concerned that this policy has not been fully implemented across the IC.

The Committee supports substantially enhancing and expediting efforts to deter the insider threat. The Committee believes that addressing the insider threat requires an integrated counterintelligence and security apparatus that spans the IC and the U.S. Government. Stovepiping counterintelligence and security capabilities can prevent derogatory information about personnel from being shared and allow spies and others seeking to disclose classified national security information to roam undetected in the Community. The Committee believes the IC's information technology modernization effort—the IC Information Technology Enterprise—must provide the infrastructure to detect insider threats earlier and more effectively. Robust counterintelligence data and analytic tools to monitor, analyze and audit personnel behavior will be critical to this endeavor.

Under current law, the IC is required to have a fully operable automated insider threat detection system in place by the end of Fiscal Year 2014. In this bill and associated classified annex, the Committee has recommended additional resources to help assure the IC meets this and other counterintelligence and security goals as soon as possible.

Action on R&D Commission findings

In June 2013, the bipartisan National Commission for the Review of the Research and Development Programs of the United States Intelligence Community issued its report to Congress, as required by Public Law 107–306. The commission identified a number of concerns, many of which have been surfaced in previous studies (dating to the 1948 Eberstadt Report) and been the subject of past reform efforts (including the Intelligence Reform and Terrorism Prevention Act of 2004). Most notably, the commission found the continued inability of the IC to confidently estimate research and development (R&D) investments across the various agencies and elements (e.g., cyber R&D), which would enable smarter spending in today's constrained budget environment. Being able to identify R&D investments is a baseline requirement to properly stewarding these resources. The Commission also highlighted the IC's inability to understand, let alone bring coherence to, the efforts of its various elements against foreign science and technology (known as S&TI). S&TI informs not only IC R&D investment decisions, but also policymakers' decisions about what capabilities to develop. The IC's R&D and S&TI capabilities are only growing in importance given the pace and scope of change in technology and the threat environment.

Therefore, within 180 days of enactment, the DNI, in conjunction with the Under Secretary of Defense for Intelligence (USD(I)), shall provide a Zero Based Review to the congressional intelligence committees. This Zero Based Review shall include the following:

- The identification of total financial investments for R&D functions and programs allocated across the NIP and Military Intelligence Program (MIP), and their relationship to investments at other U.S. Government departments and agencies;
- An explanation of the requirements process for S&TI across the IC, including identifying similarities and differences in procedure and nomenclature across the various agencies and elements;
- A review of current organization, to include IC leadership and management of R&D and S&TI efforts across the IC and within each agency, for how the IC attains synergies and unity of effort, and how it avoids unnecessary duplication of R&D.

The Committee also believes a strategic plan for R&D and S&T is essential to meeting the challenges of a globalized, interconnected world. The rapid diffusion of science and technology across the globe provides state and non-state actors with new opportunities to develop asymmetric advantages, increasing the risk of strategic surprise to the U.S. Government. From advanced manufacturing to advanced biometrics, we cannot take for granted legacy superiority in technology and expect the United States to maintain its competitive edge. The unique nature of science and technology requires a renewed commitment from senior leaders within the IC, especially at a time when neither R&D nor S&TI attracts sufficient prioritization from policymakers in the executive and legislative branches of government.

Therefore, the Committee directs the DNI, in conjunction with USD(I), to append a Strategic Plan to the Fiscal Year 2015 congressional budget submission. The plan shall include both the NIP and MIP. The Strategic Plan must include mechanisms to:

- Establish robust leadership, unity of effort, and an emphasis on R&D issues;
- Establish an executive agent within the IC for S&TI;
- Better align R&D investments across the IC in order to avoid unnecessary duplication and to achieve synergies among R&D efforts across the NIP and MIP;
- Develop partnerships with, and leverage talent from, academia and industry, especially smaller, innovative firms that may not traditionally collaborate or contract with the U.S. Government, and an R&D reserve corps to supplement the IC's expertise as needed;
- Increase policymakers' exposure to global R&D trends that could affect U.S. national security or undermine the U.S. Government's R&D efforts;
- Leverage the foreign scientific and technical talent increasingly available to U.S. academic institutions and businesses.

Analysis of commercial imagery capabilities

In our increasingly constrained budget environment, the Committee is committed to reducing the costs of acquiring electro-optical and radar satellite imagery to meet the requirements of our nation's leaders, military forces and other mission partners.

Imagery obtained from the commercial satellite industry has several virtues, including supporting IC and Department of Defense missions that require sharing unclassified imagery products with foreign or other government partners, and assisting first-responders during natural disasters such as floods or forest fires. In addition, it may be more cost-effective, depending on specific capabilities on orbit. The Committee supports commercial imagery and believes industry proposals to further enhance the capabilities of commercial data providers are worthy of additional discussion.

Leveraging commercial imagery and radar is in line with longstanding policy guidance. The U.S. Commercial Remote Sensing Policy (April 2003) states, "the United States Government will rely to the maximum practical extent on U.S. commercial remote sensing space capabilities for filling imagery and geospatial needs for military, intelligence, foreign policy, homeland security and civil users." The National Space Policy (Presidential Policy Directive 4, June 2010) directs the Executive branch to, "Purchase and use commercial space capabilities and services to the maximum practical extent when such capabilities and services are available in the marketplace and meet the U.S. Government's requirements [and] modify commercial space capabilities and services to meet government requirements when existing commercial capabilities and services do not fully meet these requirements and the potential modification represents a more cost-effective and timely acquisition approach for the government." The DNI's and Secretary of Defense's "Electro-Optical Way Ahead" strategy (approved on April 7, 2009) combined high-resolution government satellites and enhanced use of mid-resolution commercial systems and called for increasing the use of imagery available through U.S. commercial providers.

More generally, Part 10 of the Federal Acquisition Regulation favors commercial solutions, requiring government agencies, before any major acquisition, to conduct market research, "To determine if commercial items or, to the extent commercial items suitable to

meet the agency's needs are not available, non-developmental items are available that meet the agency's requirements, could be modified to meet the agency's requirements, or could meet the agency's requirements if those requirements were modified to a reasonable extent."

Pursuant to the Intelligence Authorization Act of Fiscal Year 2013, the Committee impaneled an independent GEOINT Commission, whose mandate was to examine the entire scope of the nation's GEOINT architecture, including its performance, ability to meet mission requirements, and affordability. The commission's findings echo a need to closely examine current utilization of commercial satellite imagery.

Therefore, the Committee directs the DNI and the Secretary of Defense to conduct an analysis to determine: (1) which national and military intelligence mission requirements can be satisfied with current or proposed architectures from the commercial electro-optical and radar imagery satellite industry; (2) whether long-term service level agreements (i.e., 10 years or longer) with commercial providers would be more cost effective in meeting mission requirements than future government-owned constellations of the same or similar systems; and (3) whether greater reliance on commercial systems may provide certain benefits (e.g., greater resiliency, easier replacement, risk-sharing with the private sector, and greater ability to share unclassified imagery with others) or encumber certain risks. This analysis should inform decisions about the amount and mix of National Technical Means and commercially available imagery that the IC should invest in in the future that balances meeting mission requirements and cost. This analysis should be presented to the Committee no later than 90 days after the enactment of this legislation.

Commercial imagery

The Committee understands that a commercial data provider has requested licensing approval to collect and sell on the open market, electro-optical imagery with a ground sample distance of 0.25-meter. Recognizing the ability of U.S. commercial imagery providers to contribute more substantially to the national security mission at a lower cost point, and consistent with the U.S. policy of enabling U.S. companies to maintain a leadership position in this industry, the Committee encourages the GEOINT functional manager and the DNI to promptly review this licensing request. The Committee is concerned that foreign commercial imagery providers may soon be able to provide imagery at or better than the currently allowed commercial U.S. resolution limit of 0.5 meters. As foreign firms approach or surpass this level of resolution, current restrictions on U.S. commercial imagery data providers put the United States at a competitive disadvantage and may harm an industrial base that is important to national security.

Cross-intelligence cost and effectiveness report

In a time of tightening budgets for the IC, the Committee requires accurate and detailed data on the effectiveness of all of the intelligence disciplines given the anticipated missions the IC will face, relative to their costs to the taxpayer, in order to effectively legislate and authorize expenditures for the NIP.

Therefore, the Committee directs the ODNI to complete a detailed analysis comparing the effectiveness and costs of the Geospatial, Human, Measurement and Signatures, Open Source, and Signals Intelligence disciplines. The study must include detailed analysis of the costs and effectiveness of subcomponents and major programs of each intelligence discipline. The DNI shall provide a written report and oral brief covering this analysis to the Committee no later than 90 days after the enactment of this legislation.

Intelligence Community Science, Technology, Engineering and Mathematics workforce needs

The IC's long-term success in a highly competitive security landscape will depend on a workforce that has significant expertise in the science, technology, engineering and mathematics (STEM) disciplines. The Committee supports workforce recruitment efforts to create pipelines of STEM-trained students from our nation's universities. Such efforts may include fellowships, summer internships, semester externships, and sponsored-research. The Committee is aware of interest in such program at some of the IC's technically focused elements, including NRO. The IC's Centers for Academic Excellence, for which the DIA is the executive agent, and the NSA's Cyber Center for Academic Excellence may offer models and a set of best practices that can be applied to the STEM student population. The Committee also is aware of a STEM coop program that involves an initial group of schools, including the University of Southern California, University of Nevada at Las Vegas, Mississippi State University and Auburn University, that has promise.

Therefore, the Committee encourages the IC's human capital officers and their mission partners to develop and invest in programs that are designed to attract a large pool of STEM students from the full geographic diversity of U.S. academic institutions. These programs should have cost-effective operating models and demonstrate clear benefit to the IC. The Committee also requests briefings on such initiatives.

Intelligence Advanced Research Projects Activity (IARPA)

The Committee continues to strongly support the mission of the Intelligence Advanced Research Projects Activity (IARPA), which focuses on high-risk, high-reward research and development to help the IC meet a dynamic and rapidly changing security and threat environment. IARPA's mission should remain a priority, even during the fiscal environment when research and development investment can come under pressure. Its mission and work should be integral to the IC R&D strategic plan required above.

Therefore, the Committee strongly supports full preservation of the budget request for IARPA in Fiscal Year 2014 and encourages robust investment by the IC in IARPA in Fiscal Year 2015.

Presidential appointment and Senate confirmation of positions within the Intelligence Community

In S. 1681, the Committee provides for the direct Senate confirmation of four positions—the Director of the NSA, the Inspector General of the NSA, the Director of the NRO, and the Inspector General of the NRO. The Committee believes that Senate confirma-

tion of these four positions will improve oversight and accountability and, ultimately, the effectiveness of the agencies in question. While the Committee supports Senate confirmation of these four positions, the Committee also believes that it is necessary to reduce the overall number of positions subject to Senate confirmation across the government. Therefore, the Committee will evaluate whether there are other positions within the IC that are currently subject to Senate confirmation that do not continue to require Senate advice and consent. The Committee also is cognizant of the need to ensure that critical leadership positions within the IC do not remain vacant as a result of a lengthy appointment or confirmation processes.

National Security threat assessments

The Committee has an interest in reviewing intelligence assessments prepared by the IC as part of the Committee on Foreign Investment in the United States (CFIUS) process and has reached an agreement with the ODNI and Senate Banking Committee on this matter.

Under this agreement, upon completion of a review or investigation that concludes CFIUS action, or the announcement by the President of a decision, for a covered transaction, the DNI will alert the congressional intelligence committees to the availability of any National Security Threat Assessment (NTSA) completed by the IC. These alerts will occur on a biweekly basis, will be included in the "National Intelligence Council (NIC) Weekly," and shall include the title of the NSTA, foreign company host country, date of publication, and short summary. Further, the DNI shall provide a briefing on any NSTA and the NSTA itself upon request by the congressional intelligence committees.

COMMITTEE ACTION

On November 5, 2013, 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 the base text for purposes of amendment. The Committee also authorized the staff to make technical and conforming changes in the bill, report, and annex, following the completion of the mark-up.

By unanimous consent, the Committee agreed to a managers' amendment by Chairman Feinstein and Vice Chairman Chambliss to: (1) strike a provision from the bill concerning Committee access to reports and assessments produced as part of the CFIUS process and replace it with language in the report to accompany the bill; (2) require IC elements to submit plans to Congress concerning plans for orderly shutdown in the event of a lapse in appropriations; (3) require reports on the Syrian chemical weapons program; (4) require Senate confirmation of the Director of the NSA and the Inspector General of the NSA; (5) amend the whistleblower title to add protection for whistleblower disclosures made to Inspectors

General within the IC and to the congressional intelligence committees; and (6) to make amendments to the classified annex.

By a vote of 8 ayes to 7 noes the Committee agreed to an amendment by Senator Feinstein to require the President to make public an annual report on the number of combatants and noncombatant civilians killed or injured by the use of targeted lethal force. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Coburn—no.

By a vote of 10 ayes to 5 noes the Committee agreed to an amendment by Senator King to require independent alternative analysis of the analytic basis for use of targeted lethal force against a United States person. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—aye; Senator Collins—aye; Senator Coburn—no.

By a vote of 6 ayes to 9 noes the Committee rejected an amendment offered by Senator Feinstein to substitute with report language the text of an amendment offered by Senator Coburn to make the Director and Inspector General of the NRO subject to Senate confirmation. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—no; Senator Mikulski—aye; Senator Udall—no; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—no; Senator Burr—no; Senator Risch—no; Senator Coats—no; Senator Rubio—no; Senator Collins—no; Senator Coburn—no.

By a vote of 14 ayes to 0 noes the Committee agreed to the amendment by Senator Coburn to make the Director and Inspector General of the NRO subject to Senate confirmation. The votes on the amendment in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—did not vote; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—aye; Senator Burr—aye; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Coburn—aye.

Vote to report the committee bill

The Committee voted to report the bill, as amended, by a vote of 13 ayes and 2 noes. The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Mikulski—aye; Senator Udall—aye; Senator Warner—aye; Senator Heinrich—aye; Senator King—aye; Vice Chairman Chambliss—aye; Senator Burr—no; Senator Risch—aye; Senator Coats—aye; Senator Rubio—aye; Senator Collins—aye; Senator Coburn—no.

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 November 7, 2013, the Committee transmitted this bill to the Congressional Budget Office and requested an estimate of the costs incurred in carrying out the unclassified provisions.

EVALUATION OF REGULATORY IMPACT

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

CHANGES IN EXISTING LAWS

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.

○