

## Calendar No. 120

111TH CONGRESS }  
*1st Session* }

SENATE

{ REPORT  
111-55

---

---

### INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2010

—————  
JULY 22, 2009.—Ordered to be printed  
—————

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

### R E P O R T

together with

### ADDITIONAL VIEWS

[To accompany S. 1494]

The Select Committee on Intelligence, having considered an original bill (S. 1494) to authorize appropriations for fiscal year 2010 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

#### CLASSIFIED ANNEX TO THE COMMITTEE REPORT

The classified nature of United States intelligence activities precludes disclosure by the Committee of details of its budgetary recommendations. The Committee has prepared a classified annex to this report that contains a classified Schedule of Authorizations. The 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 of 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 2010 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 2010.

*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 (expressed as full-time equivalent positions) for fiscal year 2010 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 Director of National Intelligence (DNI) in managing the civilian personnel of the Intelligence Community. Section 103(a) provides that the DNI may authorize employment of civilian personnel (expressed as full-time equivalent positions) in fiscal year 2010 in excess of the number of authorized full-time equivalent positions by an amount not exceeding 5 percent (rather than the 2 percent in prior law) of the total limit applicable to each Intelligence Community element under Section 102. The DNI may do so only if necessary to the performance of important intelligence functions.

Section 103(b) provides additional flexibility when the heads of Intelligence Community elements determine that work currently performed by contract personnel should be performed by government employees. It does so by authorizing the DNI to authorize employment of additional full-time equivalent personnel in a number equal to the number of full-time equivalent contract personnel currently performing that work. The initial exercise of this authority must be reported in advance to the congressional intelligence committees. The Committee expects this authority to be implemented in accordance with a plan that includes adequate support for personnel. Exercise of this authority should result in an actual reduction of the number of contract personnel and not a shift of resources to hire other contract personnel.

During consideration of the fiscal year 2008 request, the congressional intelligence committees learned that practices within different elements of the Intelligence Community on the counting of personnel with respect to legislatively-fixed ceilings were inconsistent, and included not counting certain personnel at all against personnel ceilings. The committees requested that the Intelligence Community Chief Human Capital Officer (IC CHCO) ensure that by the beginning of fiscal year 2010 there would be a uniform and

accurate method of counting all Intelligence Community employees under a system of personnel levels expressed as full-time equivalents. The committees also expressed their view that the DNI express the personnel levels for civilian employees of the Intelligence Community as full-time equivalent positions in the congressional budget justifications for fiscal year 2010. The DNI has done so. In addition, the IC CHCO and the Chief Financial Officer issued guidance in 2008 to ensure a uniform method for counting Intelligence Community employees. Section 103(c) directs the DNI to establish formal guidance, including exemptions from personnel levels, for student, reserve corps, joint duty, long-term training and similar programs.

In prior years the DNI has stated that statutory personnel ceilings have led to the increased use of contract personnel and have hindered the Intelligence Community's civilian joint duty, student employment, and National Intelligence Reserve Corps programs. The DNI has requested the flexibility to manage personnel levels according to budget resources rather than subject to fixed personnel numbers set for the end of the fiscal year. The DNI has stressed that no major departments in the U.S. government are subjected to statutory civilian personnel ceilings. In the Administration's request for legislative authorities as part of the Intelligence Authorization Act for Fiscal Year 2010, the DNI again requested the authority to manage personnel levels according to budget resources and in addition, for the first time, requested a legislative provision, similar to 10 U.S.C. 129, which would prohibit legislatively-fixed civilian end-strength personnel ceilings on the Intelligence Community.

In general, the Committee is supportive of eliminating fixed personnel ceilings on the number of Intelligence Community civilian personnel in order to enable the Intelligence Community to manage to budget beginning in fiscal year 2011. The Committee has not adopted this legislative priority of the DNI at this time, however, in light of the fact that the IC CHCO is currently undertaking a study of the overall civilian personnel requirements for the Intelligence Community, which is expected to be completed in September 2009. The Committee believes there should be an analysis of the overall long-term personnel requirements of the Intelligence Community before the personnel ceiling requirement is removed. The Committee also requests that the DNI provide, in support of the fiscal year 2011 budget request, information about how full-time equivalent or other employment measurements will be used as a budgetary planning tool, and for administrative controls on personnel decisions, even if Congress determines to lift express statutory limits on personnel numbers in favor of management-to-budget.

#### *Section 104. Intelligence Community Management Account*

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the DNI and sets the authorized full-time equivalent personnel levels for the elements within the ICMA for fiscal year 2010.

Subsection (a) authorizes appropriations of \$786,812,000 for fiscal year 2010 for the activities of the ICMA. Subsection (b) authorizes 792 full-time equivalent personnel for elements within the

ICMA for fiscal year 2010 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) provides that personnel level flexibility available to the DNI under Section 103 is also available to the DNI in adjusting personnel levels within the ICMA. Subsection (d) authorizes additional appropriations and full-time equivalent personnel 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, 2011.

*Section 105. Restriction on conduct of intelligence activities*

Section 105 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.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT  
AND DISABILITY SYSTEM

*Section 201. Authorization of appropriations*

Section 201 authorizes appropriations in the amount of \$290,900,000 for fiscal year 2010 for the Central Intelligence Agency (CIA) Retirement and Disability Fund.

*Section 202. Technical modification to mandatory retirement provision of the Central Intelligence Agency Retirement Act*

Section 202 updates the CIA Retirement Act to reflect the Agency's use of pay levels rather than pay grades within the Senior Intelligence Service.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Subtitle A—Personnel Matters

*Section 301. Increase in employee compensation and benefits authorized by law*

Section 301 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 302. Enhanced flexibility in details to elements of the Intelligence Community*

Section 302 extends from one year to up to three years the length of time that United States Government personnel may be detailed to the staff of an element of the Intelligence Community funded through the National Intelligence Program from another element of the Intelligence Community or from another element of the United States Government on a reimbursable basis or non-reimbursable basis, under which the employee continues to be paid by the sending agency. To utilize this authority, the joint agreement of the head of the receiving element and the head of the detailing element

(or the designees of such officials) is required. This authority will provide flexibility for elements of the Intelligence Community to receive support from other elements of the United States Government for community-wide activities where both the agencies would benefit from the detail. The DNI is seeking this authority primarily in aid of the Intelligence Community's Joint Duty Program which Congress has mandated to foster the development of personnel who have broad Intelligence Community experience and perspective. Joint duty assignments are from one to three years in length. The ability to provide for details of up to three years is therefore important in assisting in the achievement of the goals of the Joint Duty Program.

*Section 303. Enhancement of authority of the Director of National Intelligence for flexible personnel management among the elements of the intelligence community*

Section 303 adds three subsections to Section 102A of the National Security Act of 1947, to promote the DNI's ability to manage the elements of the Intelligence Community as a single cohesive community.

Subsection 102A(s) enables the DNI, with the concurrence of a department or agency head, to convert competitive service positions and incumbents within an Intelligence Community element to excepted positions. In requesting this authority, the DNI points out that because of their unique intelligence, investigative, and national security missions, most Intelligence Community elements are in the excepted civil service. However, civilian employees in several smaller Intelligence Community elements are still covered under competitive service rules. The ability to convert those positions to the excepted service will enable the DNI to establish a more uniform system throughout the Intelligence Community that will improve personnel flexibility and be responsive to the need for secrecy. Subsection 102A(s) additionally allows the DNI to establish the classification and ranges of rates of basic pay for positions so converted.

Subsection 102A(t) provides enhanced pay authority for critical positions in portions of the Intelligence Community where that authority does not now exist. It allows the DNI, in consultation with the Director of the Office of Management and Budget (OMB) and the Director of the Office of Personnel Management (OPM), to authorize the head of a department or agency with an Intelligence Community element to fix a rate of compensation in excess of applicable limits with respect to a position that requires an extremely high level of expertise critical to accomplishing an important mission and to the extent necessary to recruit or retain an exceptionally well-qualified individual for the position. A rate of pay higher than Executive Level II would require written approval of the DNI. A rate of pay higher than Executive Level I would require written approval of the President in response to a DNI request.

Subsection 102A(u) grants authority to the DNI to authorize Intelligence Community elements, with concurrence of the concerned department or agency head and in coordination with the Director of the OPM, to adopt compensation, performance management, and scholarship authority that have been authorized for any other Intelligence Community element if the DNI determines that the

adoption of such authority would improve the management and performance of the Intelligence Community and notice is provided to the congressional intelligence committees no later than 60 days in advance of adoption of the authority.

*Section 304. Award of rank to members of the Senior National Intelligence Service*

Section 304 adds another new subsection to Section 102A of the National Security Act of 1947. Subsection 102A(v) authorizes Presidential Rank awards to members of the Senior National Intelligence Service (SNIS) and other Intelligence Community senior civilian officers not already covered by such a rank award program.

According to the DNI, the authority to issue Presidential Rank Awards was originally enacted in 1978 as a program of the Senior Executive Service (SES), to honor high-performing senior career employees. The CIA and other elements of the Intelligence Community were exempted by statute from the SES, and thus not eligible for Presidential Rank Awards. Legislation enacted since 1978 has opened the eligibility for Presidential Rank Awards to senior civilian officers of exempt agencies, including the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, and members of the Defense Intelligence Senior Executive Service. This legislation would authorize the President to recognize members of the SNIS and other senior civilian officers not already covered by such a program who deserve such recognition with Presidential Rank, in a manner consistent with rank awards conferred on other senior executives of the Executive Branch.

*Section 305. Annual personnel level assessments for the Intelligence Community*

Section 305 adds a new Section 506B to Title V of the National Security Act of 1947 (50 U.S.C. 413 et seq.), an oversight mechanism that requires the DNI to conduct, in consultation with the head of the element of the Intelligence Community concerned, an annual personnel level assessment for each of the elements within the Intelligence Community and provide those assessments with the submission of the President's budget request each year.

The assessment consists of four parts. First, the assessment must provide basic personnel and contract personnel information for the concerned element of the Intelligence Community (with government personnel expressed as full-time equivalent positions) for the upcoming fiscal year. It requires that the data be compared against current fiscal year and historical five-year numbers and funding levels. Second, the assessment must include a written justification for the requested funding levels. This requirement is necessary to ensure that any personnel cost cuts or increases are fully documented and justified. Third, the assessment must contain a statement by the DNI that, based upon current and projected funding, the concerned element will have the internal infrastructure, training resources, and sufficient funding to support the administrative and operational activities of the requested civilian and contract personnel levels. Finally, the assessment must contain a list of all contract personnel who have been the subject of an investigation by the inspector general of any element of the Intelligence

Community during the previous fiscal year or who are or have been the subject of an investigation during the current fiscal year.

The Committee believes that the personnel level assessment tool is necessary for the Executive branch and Congress to fully understand the consequences of managing the Intelligence Community's personnel levels, particularly in light of a transition to managing personnel according to available funds. In recent years, the Committee has been concerned that the sharp growth in personnel numbers after the terrorist attacks on September 11, 2001, was unsustainable. In particular, when overall budgets do not keep pace with inflation and decline in real terms, personnel costs as a percentage of the budget increase each year and divert funds from operations and modernization.

Another longstanding concern of the Committee has been the Intelligence Community's increasing reliance upon contract personnel to meet mission requirements. The Committee has taken steps to reduce this reliance upon contract personnel that are described in the classified annex, as well as in the authority for contract personnel conversion in Section 103. The Committee believes that the annual personnel level assessment tool will assist the DNI and the elements of the Intelligence Community in arriving at an appropriate balance of contract personnel and permanent government employees.

With regard to historical contract personnel levels to be included in the annual assessments, the DNI has expressed concern that there was no completed effort, prior to the ODNI's contract personnel inventory initiated in June 2006, to comprehensively capture information on the number and costs of contract personnel throughout the Intelligence Community. Because of the concerns outlined by the DNI, the Committee understands that the information about contract personnel levels prior to June 2006 may need to be reported as a best estimate.

*Section 306. Temporary personnel authorizations for critical language training*

Section 306 contains findings regarding the continuing lack of critical language-capable personnel in the Intelligence Community, and the need to address this shortage through improved training for current employees, in addition to recruitment of new employees with these skills. It notes that existing personnel ceilings can make it difficult to send employees to get critical language training because individuals absent for long-term training can still count as part of an authorized personnel total, making it difficult to replace them while they are gone.

Section 306 addresses this problem by giving the DNI the authority to transfer full-time equivalent positions to elements of the Intelligence Community on a temporary basis, to enable these elements to replace individuals who are participating in long-term language training, or to accept temporary transfers of language-capable employees from other elements of the Intelligence Community. This provision complements Section 103, which authorizes the DNI to issue guidance on the treatment of personnel under personnel ceilings, to include exemptions from personnel ceilings for personnel engaged in long-term full-time training. Section 306 authorizes an additional 100 full-time equivalent positions for the

ODNI, and notes that these positions are to be used specifically to implement the new authorities granted by this section.

Section 306 refers to “critical foreign language training,” rather than “foreign language training.” The Committee understands that this phrasing will permit the DNI to use this new authority in situations where an employee of the Intelligence Community who speaks English as a second language needs further training in English, in order to comprehend particular complex or technical subjects.

#### Subtitle B—Education Programs

##### *Section 311. Permanent authorization for the Pat Roberts Intelligence Scholars Program*

Section 311 provides a permanent authorization for the Pat Roberts Intelligence Scholars Program (PRISP), which was originally authorized as a pilot program in Section 318 of the Intelligence Authorization Act for Fiscal Year 2004 and has continued under year-to-year appropriations. In addition, Section 311 would authorize the broader use of PRISP funds beyond intelligence analysts to include acquisition, science and technology, and other intelligence professionals, thus allowing the program to be used to develop the Intelligence Community workforce across a range of disciplines. Section 311 also authorizes the use of funds to allow students participating in the program to receive funds for books, travel expenses and a stipend.

The PRISP has provided education funds to over 800 individuals since its inception in 2004, with an attrition of less than one percent of program participants. Intelligence agencies have been supportive of the program as it provides them the flexibility to compete effectively with the private sector to recruit individuals who possess critical skills sought by the Intelligence Community.

##### *Section 312. Modifications to the Louis Stokes Educational Scholarship Program*

Section 16 of the National Security Agency Act of 1959 (50 U.S.C. 402 note) authorizes the National Security Agency (NSA) to establish an undergraduate training program to facilitate recruitment of individuals with skills critical to its mission. The program is known as the Stokes Educational Scholarship Program, named for Representative Louis Stokes, a former chairman of the Permanent Select Committee on Intelligence of the U.S. House of Representatives.

Section 312 is intended to expand and strengthen the Stokes program. Section 312(a) expands the Stokes program to authorize the inclusion of graduate students. Section 312(e) amends Section 16 to permit the NSA Director to protect intelligence sources and methods by deleting a requirement that NSA publicly identify to educational institutions students who are NSA employees or training program participants. Deletion of this disclosure requirement will enhance the ability of NSA to protect personnel and prospective personnel and to preserve the ability of training program participants to undertake future clandestine or other sensitive assignments for the Intelligence Community.



The Committee recognizes that nondisclosure is appropriate when disclosure would threaten intelligence sources or methods, would endanger the life or safety of the student, or would limit the employee's or prospective employee's ability to perform intelligence activities in the future. Notwithstanding the deletion of the disclosure requirement, the Committee expects NSA to continue to prohibit participants in the training program from engaging in any intelligence functions at the institutions they attend under the program. *See* H.R. Rep. No. 99-690, Part I (1986) ("NSA employees attending an institution under the program will have no intelligence function whatever to perform at the institution.").

Section 312 is also intended to make the program more effective by clarifying that "termination of employment" includes situations where employees fail to maintain satisfactory academic standards. According to the DNI, failure to maintain satisfactory academic performance has always been grounds for default resulting in the right of the government to recoup educational costs expended for the benefit of the defaulting employee. Section 312(c) would also expand the program by authorizing NSA to offer participation in the Stokes program to individuals who are not current federal employees.

Finally, Section 312(e) authorizes other intelligence agencies to establish undergraduate or graduate training program for civilian employees or prospective civilian employees that are similar to programs under Section 16 of the National Security Agency Act.

*Section 313. Intelligence officer education programs*

Section 313 authorizes the Intelligence Officer Training Program (IOTP), which builds on two pilot programs that were authorized in previous years: the NSA "Pilot Program on Cryptologic Service Training," described in Section 922 of the Defense Authorization Act for Fiscal Year 2005, Public Law 108-375 (2004) (50 U.S.C. 402 note), and the Director of Central Intelligence pilot program "Improvement of Equality of Employment Opportunities in the Intelligence Community," under Section 319 of the Intelligence Authorization Act for Fiscal Year 2003, Public Law 108-177 (2003) (50 U.S.C. 403 note). The purpose of the IOTP is to encourage the preparation, recruitment, and retention of civilian personnel for careers in the Intelligence Community. It is also to help ensure that the Intelligence Community can better recruit and retain a workforce that is ethnically and culturally diverse so that it can accomplish its critical national security mission.

The program is to consist of two parts. First, the program would provide financial assistance to individuals through existing Intelligence Community scholarship authorities to pursue studies in critical language, analytic, scientific, technical, or other skills necessary to meet current or emerging needs of the Intelligence Community. Second, building on the ODNI's successful Centers for Academic Excellence program, IOTP is to solicit colleges and universities from across the country to apply for grants on a competitive basis to implement academic programs which will help students develop the critical skills needed for careers in the Intelligence Community.

Students attending participating colleges and universities and taking the prescribed course of study may competitively apply for

financial assistance including, but not limited to, a monthly stipend, tuition assistance, book allowances, and travel expenses. Students who receive a threshold amount of assistance are obligated to serve in the Intelligence Community. The ODNI is to develop application requirements for students, which could include the successful completion of a security background investigation.

Section 313 makes permanent an NSA pilot program that provided grants to academic institutions. The original NSA pilot program, with its focus on cryptologic service at NSA, although beneficial to NSA, no longer meets the variety of the Intelligence Community's critical skills requirements. The IOTP, with its broader scope, is intended to assist the Intelligence Community in establishing and building partnerships with academic institutions and ensure a continuous pool of qualified entry-level applicants to Intelligence Community elements, tailored to changing priorities of an evolving Intelligence Community enterprise.

Section 313 repeals the authorizations for the following programs that are either incorporated into or replaced by the IOTP: the pilot program authorized by Section 319 of the Intelligence Authorization Act for Fiscal Year 2004, Public Law 108-177 (2003) (50 U.S.C. 403 note); the scholarship program authorized by Section 1043 of the Intelligence Reform and Terrorism Prevention Act, Public Law 108-458 (2004) (50 U.S.C. 441g-2) (Intelligence Reform Act); and the pilot program authorized by Section 922 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Public Law 108-375 (50 U.S.C. 402 note).

*Section 314. Review and report on education programs*

Section 314 requires the DNI to review and report on whether the Pat Roberts Intelligence Scholars Program, the Louis Stokes Educational Scholarship Program, the Intelligence Officer Training Program authorized under Section 313, and any other Intelligence Community education programs are meeting the needs of the Intelligence Community to prepare, recruit, and retain a skilled and diverse workforce, and whether they should be combined or otherwise integrated. The DNI is to submit the report to the congressional intelligence committees by February 1, 2010.

Subtitle C—Acquisition Matters

*Section 321. Vulnerability assessments of major systems*

Section 321 adds a new Section 506C to the National Security Act of 1947. This provision creates an oversight mechanism that requires the DNI to conduct an initial vulnerability assessment and subsequent assessments of every major system and its significant items of supply in the National Intelligence Program. The intent of the provision is to provide Congress and the DNI with an accurate assessment of the unique vulnerabilities and risks associated with each National Intelligence Program major system to allow a determination of whether funding for a particular major system should be modified or discontinued. The vulnerability assessment process will also require the various elements of the Intelligence Community responsible for implementing major systems to give due consideration to the risks and vulnerabilities associated with such implementation.

Section 321 requires the DNI to conduct an initial vulnerability assessment on every major system and its significant items of supply proposed for the National Intelligence Program prior to completion of Milestone B or an equivalent acquisition decision. The minimum requirements of the initial vulnerability assessment are fairly broad and intended to provide the DNI with significant flexibility in crafting an assessment tailored to the proposed major system. Thus, the DNI is required to use, at a minimum, an analysis-based approach to identify vulnerabilities, define exploitation potential, examine the system's potential effectiveness, determine overall vulnerability, and make recommendations for risk reduction. The DNI is obviously free to adopt a more rigorous methodology for the conduct of initial vulnerability assessments.

Vulnerability assessments should continue through the life of a major system and its significant items of supply. Numerous factors and considerations can affect the viability of a given major system. For that reason, Section 321 provides the DNI with the flexibility to set a schedule of subsequent vulnerability assessments for each major system when the DNI submits the initial vulnerability assessment to the congressional intelligence committees. The time period between assessments should depend upon the unique circumstances of a particular major system. For example, a new major system that is implementing some experimental technology might require annual assessments while a more mature major system might not need such frequent reassessment. The DNI is also permitted to adjust a major system's assessment schedule when the DNI determines that a change in circumstances warrants the issuance of a subsequent vulnerability assessment. Section 321 also provides that the DNI may conduct a subsequent vulnerability assessment of a major system when requested to do so by a congressional intelligence committee.

The minimum requirements for a subsequent vulnerability assessment are almost identical to those of an initial vulnerability assessment. There are only two additional requirements. First, if applicable to the given major system during its particular phase of development or production, the DNI must also use a testing-based approach to assess the system's vulnerabilities. Obviously, common sense needs to prevail here. For example, the testing approach is not intended to require the "crash testing" of a satellite system. Nor is it intended to require the DNI to test system hardware. However, the vulnerabilities of a satellite's significant items of supply might be exposed by a rigorous testing regime. Second, the subsequent vulnerability assessment is required to monitor the exploitation potential of the major system. Thus, a subsequent vulnerability assessment should monitor ongoing changes to vulnerabilities and understand the potential for exploitation. Since new vulnerabilities can become relevant and the characteristics of existing vulnerabilities can change, it is necessary to monitor both existing vulnerabilities and their characteristics, and to check for new vulnerabilities on a regular basis.

Section 321 requires the DNI to give due consideration to the vulnerability assessments prepared for the major systems within the National Intelligence Program. It also requires that the vulnerability assessments be provided to the congressional intelligence committees within ten days of their completion. The Committee en-

courages the DNI to share the results of these vulnerability assessments, as appropriate, with other congressional committees of jurisdiction.

Finally, the section contains definitions for the terms “items of supply,” “major system,” “Milestone B,” and “vulnerability assessment.”

*Section 322. Intelligence Community business system transformation*

A business enterprise architecture incorporates an agency’s financial, personnel, procurement, acquisition, logistics, and planning systems into one interoperable system. Historically, Intelligence Community elements have pursued unique, stovepiped systems that do not leverage the investments of other elements of the Intelligence Community. More recently there has been a more collaborative effort among the Intelligence Community elements on the development of business systems, but true transformation to an integrated Intelligence Community architecture has not been achieved.

Section 322 adds a new Section 506D to the National Security Act of 1947. It requires that the DNI create a business enterprise architecture that defines all Intelligence Community business systems, as well as the functions and activities supported by those business systems, in order to guide with sufficient detail the implementation of interoperable Intelligence Community business system solutions. The business enterprise architecture and acquisition strategy are to be submitted to the congressional intelligence committees by December 31, 2009.

Section 322 will provide the assurance that business systems that cost more than a million dollars will be efficiently and effectively coordinated. It will prohibit the obligation of appropriated funds for any system that has not been certified by the DNI either as complying with the enterprise architecture or as necessary for the national security or an essential capability. Section 322 will also require identification of all “legacy systems” that will be either terminated or transitioned into the new architecture. Further, this section will require the DNI to report to the Committee no less often than annually, for five years, on the progress being made in successfully implementing the new architecture.

*Section 323. Reports on the acquisition of major systems*

Section 323 adds a new Section 506E to the National Security Act of 1947 to require a separate report on each major system acquisition by an element of the Intelligence Community.

Among other items, the annual reports must include information about the current total acquisition cost for such system, the development schedule for the system including an estimate of annual development costs until development is completed, the planned procurement schedule for the system, including the best estimate of the DNI of the annual costs and units to be procured until procurement is completed, a full life-cycle cost analysis for such system, and the result of any significant test and evaluation of such major system as of the date of the submittal of such report. Section 323 requires that to the extent that the report is applicable to an element of the Intelligence Community within the Department of De-

fense, the report is to be submitted to the congressional armed services committees.

Section 323 includes definitions for “acquisition cost,” “full life-cycle cost,” “major contract,” “major system,” and “significant test and evaluation.”

*Section 324. Excessive cost growth of major systems*

Section 324 adds a new Section 506F to the National Security Act of 1947 to require that, in addition to the reporting required under Section 102A(q) of the Act and the amendments made by Section 323, the program manager of a major system acquisition project shall determine on a continuing basis if the acquisition cost of such major system has increased by at least 25 percent as compared to the baseline of such major system. The program manager must inform the DNI of any such determination and the DNI must submit a written notification to the congressional intelligence committees if the DNI makes the same such determination.

Section 324 is intended to mirror the Nunn-McCurdy provision in Title 10 of the United States Code that applies to major defense acquisition programs. The Committee envisions that the determination will be done as needed by the program manager of the major system acquisition and should not wait until the time that the DNI’s annual report is filed. In other words, the Committee expects the congressional intelligence committees to be advised on a regular basis by the DNI about the progress and associated costs of major system acquisitions within the Intelligence Community.

If the cost growth of a major system is 25 percent or more, the DNI must prepare a notification and submit, among other items, an updated cost estimate to the congressional intelligence committees, and a certification that the acquisition is essential to national security, there are no other alternatives that will provide equal or greater intelligence capability at equal or lesser cost to completion, the new estimates of the full life-cycle cost for such major system are reasonable, and the structure for the acquisition of such major system is adequate to manage and control full life-cycle cost of such major system.

If the program manager makes a determination that the acquisition cost has increased by 50 percent or more as compared to the baseline, and the DNI makes the same such determination, then the DNI must submit to the congressional intelligence committees a written certification of the same four items as described above, as well as an updated notification and accompanying information. The Committee also expects that if milestone authority had been delegated to the program manager, such authority would be revoked and returned to the DNI, or to the Director and Secretary of Defense, jointly, with respect to Department of Defense programs.

If the required certification, at either the 25 percent or 50 percent level, is not submitted to the congressional intelligence committees within 90 days of the DNI’s determination of cost growth, Section 324 creates a mechanism in which funds cannot be obligated for a period of time. If Congress does not act during that period, then the acquisition may continue.

With respect to major systems for which certifications are required on the date of enactment of this Act, such certifications

must be submitted within 180 days of the date of enactment. If the certification is not submitted to the congressional intelligence committees within 180 days, funds appropriated for the acquisition of the major system may not be obligated for a major contract under the program. The prohibition ceases to apply at the end of the 30-day period of a continuous session of Congress that begins on the date on which Congress receives the notification.

Section 324 requires that to the extent that the report is applicable to an element of the Intelligence Community within the Department of Defense, the report is also to be submitted to the congressional armed services committees.

*Section 325. Future budget projections*

Section 325 adds a new Section 506G to the National Security Act of 1947. It requires the DNI, with the concurrence of the OMB, to provide the congressional intelligence committees with two future budget projections that together span ten years and form the basis of affordability assessments required in this section. Section 325 thus ensures that the Intelligence Community will make long-term budgetary projections that span the same time frame as the funding needs of programs it initiates in the budget.

Section 325 requires first a Future Year Intelligence Plan for at least four years after the budget year, which includes the year-by-year funding plan for each expenditure center and for each major system in the National Intelligence Program. Section 325 also requires lifecycle cost and milestones for major systems and a Long-term Budget Projection five years beyond the Future Year Intelligence Plan, but at a much higher level of budget aggregation. This Long-term Budget Projection is to be conducted under a constrained budget projection, but under two alternative sets of assumptions about cost growth—one with virtually no cost growth, the other more in line with experience. Section 325 requires that the Long-term Budget Projection include a description of whether, and to what extent, the projection for each year for each element of the Intelligence Community exceeds the level that would result from applying the most recent OMB inflation estimate to that element. Both budget projections must be submitted to Congress with the President's budget request.

Section 325 ensures that the Executive branch and Congress will be fully aware of the long-term budgetary impact of a major system acquisition prior to its development or production. This is achieved through a requirement that prior to a major system entering Milestone A and Milestone B or an analogous stage of system development, the DNI must report to the congressional intelligence committees whether and to what extent the proposed major system will increase the Future Year Intelligence Plan and the Long-term Budget Projection for that element of the Intelligence Community. If the proposed major system is estimated to cause an increase to these future budget projections, then the DNI and OMB Director must issue a determination that the anticipated budget increase is necessary for national security.

*Section 326. National Intelligence Program funded acquisitions*

Section 326 adds a new subparagraph (4) to the acquisition authorities of the DNI collected in Section 102A(n) of the National Se-

curity Act of 1947. Existing subparagraph (1) authorizes the DNI to exercise the acquisition and appropriations authorities referred to in the Central Intelligence Agency Act of 1949 (CIA Act). Although subparagraph (1) is not explicit, those authorities are found in Sections 3 and 8 of the CIA Act, except, as provided in subparagraph (1), for the CIA's authority under section 8(b) to expend funds without regard to laws and regulations on Government expenditures for objects of a confidential, extraordinary, or emergency nature.

Subparagraph (4)(A) authorizes the DNI to make acquisition authority referred to in Sections 3 and 8(a) of the CIA Act also available to any Intelligence Community element for an acquisition that is funded in whole or in majority part by the National Intelligence Program. Among Intelligence Community elements, the National Reconnaissance Office (NRO) and the National Geospatial-Intelligence Agency (NGA) already exercise these or similar authorities either directly or through the CIA. The grant of this authority to the DNI is part of the Committee's effort to ensure that the DNI has the ability to manage the elements of the Intelligence Community as a community by enabling the DNI to make available throughout the Intelligence Community, when warranted, authority originally enacted for one of its elements.

Subparagraphs 4(B)–(G) establish procedures and controls on the grant of this authority. The head of an Intelligence Community element, without delegation, must request in writing the DNI make the authority available. The request must explain the need for the acquisition authority including an explanation why other authorities are insufficient and that the mission of the element would be impaired if the requested authority is not exercised. In turn, for the authority to be provided, the DNI, the Principal Deputy DNI, or a designated Deputy DNI must issue a written authorization that includes a justification which supports the use of the authority.

Requests from the head of an Intelligence Community element that are within the Departments of Defense, Energy, Homeland Security, Justice, State, and Treasury shall be transmitted to the DNI in accordance with procedures established by the heads of those departments. Also, to ensure periodic review, authorities may not be granted for a class of acquisitions beyond a renewable 3 years except for a renewable 6 years if the DNI personally approves the authority. The congressional intelligence committees shall be notified of all authorizations granted under subparagraph (4).

#### Subtitle D—Congressional Oversight, Plans, and Reports

##### *Section 331. General congressional oversight*

Section 331 amends the requirements for notifications to Congress under section 501 of the National Security Act of 1947 by adding a new paragraph stating that there shall be no exception to the requirements of Title V of the National Security Act of 1947 to inform the congressional intelligence committees of all intelligence activities and covert actions.

*Section 332. Improvement of notification of Congress regarding intelligence activities of the United States*

Section 332 further amends the requirements for notifications to Congress under Title V of the National Security Act of 1947. In the event the DNI or head of an Intelligence Community element does not provide to the full congressional intelligence committees the notification required by Section 502 (relating to intelligence activities other than covert actions) or Section 503 (relating to covert actions), the committees shall be provided notice of this fact. This notice must be submitted in writing in a classified form and include a description of the main features of the intelligence activity or covert action as well as a statement of the reasons for not briefing the full committee. The notice may not contain a restriction on access to it by all members of the committee.

This section also extends to Section 503 of the National Security Act of 1947 requirements now in Section 502 of the Act on the form and contents of reports. Accordingly, reports on covert actions now shall also contain a concise statement of any facts pertinent to the covert action and an explanation of the significance of the covert action. In addition, rather than the existing requirement to report changes only if they are “significant,” under the amendment any change to a covert action finding must be reported.

*Section 333. Requirement to provide legal authority for intelligence activities*

Section 333 amends the National Security Act of 1947 by requiring that the congressional intelligence committees be provided with the legal authorities under which all covert action and all other intelligence activities are or were conducted.

*Section 334. Additional limitation on availability of funds for intelligence and intelligence-related activities*

Section 334 adds to the requirements of Section 504 of the National Security Act of 1947 an enforcement mechanism for the notification provisions in Sections 501 through 503. The section provides that funds may be obligated or expended for an intelligence activity only if the congressional intelligence committees have been “fully and currently informed” of that activity. The committees will be considered to have been fully and currently informed only if all members of the committees are fully informed or, in the circumstances in which the amendments made by Section 332 apply, if the committees have been provided with a classified notice of the main features of the intelligence activity that does not contain a restriction on access by all members.

*Section 335. Audits of Intelligence Community by the Government Accountability Office*

Section 335 adds a new section to Title 31 on audits and evaluations of the Intelligence Community by the Government Accountability Office (GAO). With some modifications, it is based on S. 385, a bill entitled the “Intelligence Community Audit Act of 2009” which has been referred to the Committee.

As added by Section 335, Section 3523a(b) of Title 31 sets forth findings by Congress on the authority of the Comptroller General under present law to perform audits and evaluations of Intelligence



Community elements that are requested by committees of jurisdiction. Section 3523a(b)(2) states that requests for such audits may be made for matters relating to a list of subjects, namely, management and administration in areas such as strategic planning, financial management, information technology, human capital, and knowledge and information sharing. These are subjects on which GAO has established expertise.

In order to protect national security interests, Section 3523a(c) sets forth limitations and procedures concerning the use of this audit and evaluation authority when intelligence sources and methods or covert actions are involved. Among them are that such audits and evaluations may only be done on request of a congressional intelligence committee. The results of such audits and evaluations, or information obtained in the course of doing them, may only be provided to the congressional intelligence committees, the DNI, and the head of the relevant Intelligence Community element. It also states that GAO employees shall be subject to the same statutory penalties for unauthorized disclosure as Intelligence Community employees. Furthermore, all documents that are used during the audit or evaluation will remain in Intelligence Community facilities.

The Committee intends that the authority provided by this amendment should be used as a tool to supplement and not replace existing oversight mechanisms, in order to fill in any gaps that the congressional intelligence committees, in consultation with the DNI and Comptroller General, may identify. The Committee requests that the DNI and Comptroller General confer periodically about matters for which the GAO may properly augment oversight, and advise the congressional intelligence committees about the proposed utilization of GAO expertise.

*Section 336. Report on compliance with laws, international obligations, and Executive orders on the detention and interrogation activities of the Intelligence Community*

Section 336 requires the DNI to submit a comprehensive report to the congressional intelligence committees on all measures taken by the ODNI and by any Intelligence Community element with relevant responsibilities to comply with the provisions of applicable law, international obligations, and executive orders relating to detention or interrogation activities, including the Detainee Treatment Act of 2005 (title X of division A of Public Law 109-148) (2005), the Military Commissions Act of 2006 (Public Law 109-366) (2006), Common Article 3, the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Executive Order 13491 (74 Fed. Reg. 4893, relating to ensuring lawful interrogation) and Executive Order 13493 (74 Fed. Reg. 4901, relating to detention policy options). The report is to be submitted no later than December 1, 2009, in an unclassified form but may include a classified annex.

The Detainee Treatment Act provides that no individual in the custody or under the physical control of the United States, regardless of nationality or physical location, shall be subject to cruel, inhuman, or degrading treatment. Congress reaffirmed this mandate in Section 6 of the Military Commissions Act, adding an implementation mechanism that required the President to take action to en-

sure compliance including through administrative rules and procedures. Section 6 further provided not only that grave breaches of Common Article 3 of the Geneva Conventions are war crimes under Title 18 of the United State Code, but also that the President has authority for the United States to promulgate higher standards and administrative regulations for violations of U.S. treaty obligations. It required the President to issue those interpretations by Executive order published in the Federal Register.

The report required by Section 336 shall include a description of the detention or interrogation methods that have been determined to comply with applicable law, international obligations, and Executive order, including the prohibitions of the Detainee Treatment Act and the Military Commissions Act.

The Detainee Treatment Act also provides for the protection against civil or criminal liability for United States Government personnel who had engaged in officially authorized interrogations that were determined to be lawful at the time. Section 336 requires the DNI to report on actions taken to implement that provision. In addition, the DNI is to report on actions relating to detention or interrogation taken pursuant to Executive Order 13941 or recommendations issued by task forces established under Executive Orders 13941 and 13943.

The report shall include an appendix containing all guidelines on the application of all applicable law, international obligations, or Executive orders, including the Detainee Treatment Act and the Military Commissions Act, to the detention or interrogation activities, if any, of any Intelligence Community element. The appendix shall also include all legal justifications of the Department of Justice about the meaning or application, if applicable, of laws, international obligations, or Executive orders with respect to Intelligence Community detention or interrogation activities, if any, of any element of the Intelligence Community. The provision seeks only the legal justifications of any office of the Department of Justice that rendered an opinion on the matter.

To the extent that the report required by Section 336 addresses an element of the Intelligence Community within the Department of Defense, that portion of the report, and associated material that is necessary to make that portion understandable, shall also be submitted by the DNI to the congressional armed services committees.

*Section 337. Reports on national security threat posed by Guantanamo Bay detainees*

Section 337 requires the Intelligence Community to provide the congressional intelligence committees with a quarterly report outlining the Director of National Intelligence's assessment on the suitability of detainees previously released or transferred, or who may be released or transferred, from the Naval Detention Facility at Guantanamo Bay, Cuba to the United States or any other country. The quarterly report is to be provided in addition to, and on the same schedule as, the report on the prisoner population at the Guantanamo detention facility required by Section 319 of the Supplemental Appropriations Act of 2009 (Public Law 111-32).

The report required by Section 337 must include: (1) any objection or recommendation against the release of a particular detainee

by an element of the Intelligence Community which judged that the potential threat posed by a particular detainee warranted continued detention; (2) a detailed description of the intelligence information that led to such a determination; (3) if an element of the Intelligence Community previously recommended against the release of a particular detainee and later retracted that recommendation, a detailed explanation of the reasoning for the retraction; and (4) an assessment of lessons learned from previous releases and transfers of individuals for whom the Intelligence Community objected or recommended against release.

The intent of the provision is to allow the congressional intelligence committees to review the threat assessment and perform needed oversight in this area. The congressional intelligence committees are among the few entities that can receive this kind of detailed information, and it is the responsibility of the committees to understand the Intelligence Community's assessments of the threat, or lack thereof, posed by individual detainees as the Administration considers actions on Guantanamo detainees in the near future.

*Section 338. Report on retirement benefits for former employees of Air America*

Section 338 provides for a report by the DNI on the advisability of providing federal retirement benefits to United States citizens who were employees of Air America or an associated company prior to 1977, during the time that the company was owned or controlled by the United States and operated by the CIA.

There have been bills introduced in the Senate and House in the past that would have provided federal retirement benefits for those employees. By including Section 338 in this authorization bill, the Committee takes no position on the merits of that legislation.

Although the section invites the DNI to submit any recommendations on the ultimate question of providing benefits, the main purpose of the report is to provide Congress with the facts upon which Congress can make that determination. Accordingly, Section 338 outlines the factual elements required by the report. To aid in the preparation of the report, the section authorizes the assistance of the Comptroller General. Among the elements of the report should be: (1) the relationship of Air America to the CIA; (2) the missions it performed; (3) the casualties its employees suffered; (4) a description of the retirement benefits that had been contracted for or promised to Air America employees; and (5) a description of the retirement benefits Air America employees received.

On September 25, 2007, the CIA provided a three page letter to the congressional intelligence and appropriations committees in response to the Committee's report to accompany the Intelligence Authorization Act for Fiscal Year 2007, S. Rep. 109-259, requesting a report on "the advisability of providing federal retirement benefits to United States citizens who were employees of Air America or an associated company prior to 1977, during the time that the company was owned or controlled by the United States and operated by the CIA." Although the letter described the legal basis under current law for denying federal retirement benefits to employees of Air America, it did not provide the factual background that would allow Congress to make an assessment of whether to

amend current law to provide employees of Air America with federal retirement benefits. The report requested in Section 338 therefore continues to be necessary for a comprehensive exploration of the underlying issues.

*Section 339. Report and strategic plan on biological weapons*

Section 339 provides for a report by the DNI on the intelligence collection efforts of the United States against biological weapons or the threat of biological weapons in the hands of terrorists, rogue states, or other actors, both foreign and domestic. The report also should cover intelligence collection efforts to protect the United States bio-defense knowledge and infrastructure.

The report required by Section 339 should contain the following elements: (1) an accurate assessment of the intelligence collection efforts of the United States dedicated to detecting the development or use of biological weapons by state, non-state, or rogue actors, either foreign or domestic; (2) detailed information on fiscal, human, technical, open source, and other intelligence collection resources of the United States for use against the biological weapons threat; and (3) an assessment of any problems that may reduce the overall effectiveness of United States intelligence collection and analysis to identify and protect against biological weapons or the threat of biological weapons including intelligence collection gaps or inefficiencies, inadequate information sharing practices, or inadequate cooperation among agencies or departments of the United States.

Additionally, Section 339 provides that this report include a strategic plan prepared by the DNI that, in coordination with the Attorney General, Secretary of Defense, and Secretary of Homeland Security, provides for a coordinated action plan for the Intelligence Community to address and close the gaps identified in the report required by Section 339(a). This strategic plan shall also include a description of appropriate goals, schedules, milestones, or metrics to measure the long-term effectiveness of the plan and any long-term resource and human capital issues related to the collection of intelligence against biological weapons or the threat of biological weapons, including any recommendation to address shortfalls of experienced and qualified staff possessing relevant scientific, language, and technical skills.

Section 339 requires that the DNI submit this report to the congressional intelligence committees no later than 180 days after the enactment of this bill. The DNI is required to begin implementing the strategic plan within 30 days of submitting the report.

*Section 340. Cybersecurity oversight*

Section 340 seeks to set up a preliminary framework for executive and congressional oversight to ensure that the government's national cybersecurity mission is consistent with legal authorities and preserves reasonable expectations of privacy.

Section 340(a) defines three terms: national cyber investigative joint task force, critical infrastructure, and cybersecurity program. The definition of the term "cybersecurity programs" in section 340(a) is intentionally a narrow one. Routine firewalls and anti-virus programs, for example, might be considered cybersecurity programs. The definition of cybersecurity programs in this section intentionally excludes those types of routine programs. Instead,

Section 340 focuses on government-wide cybersecurity programs. These programs use more effective technologies to integrate cyber defenses across the government among government entities that wish to, or are directed to, participate. These types of programs pose challenging new legal and privacy questions that make congressional and Executive branch oversight particularly important. Because the section seeks to provide oversight of only those programs that involve significant potential privacy implications, the term “cybersecurity programs” is also limited by the requirement that the programs involve personally identifiable data.

Additionally, to be covered by this section, a cybersecurity program must have one of three characteristics. First, the definition covers programs in which the agency or department whose personnel is the intended recipient of the e-mail or other electronic communication uses another agency or department of the United States Government to screen personally identifiable data related to those communications. In these programs, the agency or department that is the intended recipient of the communication is not managing or operating the cybersecurity program; instead, the program is managed by a government entity like the Department of Homeland Security or the Department of Defense. Second, the definition covers programs in which personally identifiable data is transferred from the agency or department whose personnel is the intended recipient of the e-mail or other electronic communication to another agency or department for the purpose of cybersecurity. This would include, for example, programs in which tips or other results from cybersecurity operations that contain personally identifiable data are shared with law enforcement or other parts of the United States Government. Third, the definition covers programs in which personally identifiable data is transferred from the agency or department whose personnel is the intended recipient of the e-mail or other electronic communication to an element of the Intelligence Community.

Section 340(b) requires the President to notify Congress of cybersecurity programs and provide Congress with five types of documents: the program’s legal justification, any certifications of the program’s legality under 18 U.S.C. 2511(2)(a)(ii) or other statutory provision, any concept of operations, any privacy impact statement, and any plan for independent audit or review of the program to be carried out by the head of the relevant department or agency, in conjunction with the appropriate inspector general. The notification requirements of subsection (b) are designed to ensure that Congress is aware of significant legal, privacy and operational issues with respect to each new cybersecurity program. For existing cybersecurity programs, the notification and documents must be provided no later than 30 days after the date of the enactment of this Act. For new programs, the notification and documents must be provided not later than 30 days after the date of the commencement of operations of a new cybersecurity program.

Section 340(c) requires the heads of agencies or departments with responsibility for a cybersecurity program, in conjunction with the inspector general for that department or agency, to prepare a report describing the results of any audit or review under the audit plan and assessing whether the cybersecurity program is in compliance with, and adequately described by, the documents submitted

to Congress. This subsection is designed to provide an independent check that the agencies are conducting cyber operations in a manner consistent with Executive branch guidance and to supply Congress more information about the operation of those programs. In addition, these reports should help identify the key difficulties and challenges in the cybersecurity programs.

Section 340(d) requires the Inspectors General of the Department of Homeland Security and the Intelligence Community to prepare a report on the sharing of cyber threat information both within the U.S. government and with those responsible for critical infrastructure. This report should be submitted one year after the enactment of this Act. In their report, the Inspectors General should identify any barriers to sharing cyber threat and vulnerability information, and assess the effectiveness of current sharing arrangements.

Section 340(e) provides the head of an element of the Intelligence Community the authority to detail an officer or employee to the Department of Homeland Security or the National Cyber Investigative Joint Task Force to assist with cybersecurity for a period not to exceed three years. This section will allow Intelligence Community experts to be made available to the Department of Homeland Security, which serves as the civilian cyber defense manager but has not been given the same priority or funding as the Intelligence Community by the Executive branch. In recognition of this Committee's ample support for cyber over the last few years, the provision permits these details to be provided on a nonreimbursable basis. This detail authority, however, is restricted to a period not to exceed 3 years to prevent details from being used as an alternative to building expertise at civilian cyber defense agencies.

Finally, Section 340(f) provides that the requirements of this section will terminate on December 31, 2012. During the next three years, the Executive branch will begin new and unprecedented cybersecurity programs with new technology and new legal and privacy challenges. Section 340 will allow Congress to follow these developments closely and gain a deeper and broader understanding of cybersecurity issues so that, upon the termination of this section, it may be replaced with a permanent framework for oversight.

*Section 341. Sense of the Senate on a subcommittee related to intelligence appropriations*

Section 341 is a Sense of the Senate that the Senate should agree to a resolution amending Section 402 of Senate Resolution 445, 108th Congress, agreed to on October 9, 2004, as proposed in Senate Resolution 655, 110th Congress, introduced on September 11, 2008, to establish within the Committee on Appropriations of the Senate a Subcommittee on Intelligence.

S. Res. 655 outlines the key features of the Subcommittee on Intelligence. First, the Subcommittee would have exclusive jurisdiction over all funding for the National Intelligence Program. Second, no other Appropriations subcommittee could intervene to review the work of the Intelligence Subcommittee. Third, Members of the Select Committee on Intelligence who are Members of the Committee on Appropriations shall have automatic membership on the Subcommittee on Intelligence. Fourth, the Chairman and Vice Chairman of the Select Committee on Intelligence shall serve as ex-officio members of the subcommittee, if they are not also Mem-

bers of the Committee on Appropriations. Fifth, the Chairman and Ranking member of the Subcommittee on Defense of the Committee on Appropriations shall have automatic membership on the subcommittee. Finally, the Chairman and Ranking Member of the subcommittee shall be selected from among those members who are both members of the Committee on Appropriations and the Select Committee on Intelligence.

The Committee believes that the establishment of an Appropriations Subcommittee on Intelligence will provide a strong, stable, and capable congressional committee structure that will improve congressional oversight of the intelligence activities of the United States and fulfill the recommendations of the 9/11 Commission as nearly as practicable.

*Section 342. Repeal or modification of certain reporting requirements*

The Committee frequently requests information from the Intelligence Community in the form of reports, the contents of which are specifically defined by statute. The reports prepared pursuant to these statutory requirements provide this Committee 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 Intelligence Community. It is therefore important for the Congress to reconsider these reporting requirements on a periodic basis to ensure that the reports it has 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 Intelligence Community a direct line of communication to respond to congressional concerns.

In response to a request from the DNI, the Committee examined some of these recurring reporting requirements. Section 342 therefore eliminates certain reports that were particularly burdensome to the Intelligence Community when the information in the reports could be obtained through other means. It also eliminates reports whose usefulness has diminished either because of changing events or because the information contained in those reports is duplicative of information already obtained through other avenues.

Because the majority of recurring reports provide critical information relevant to the many challenges facing the Intelligence Community today, the Committee has proceeded carefully in eliminating only seven statutory reporting requirements, a very small percentage of the many recurring reports currently requested. In addition, the Committee changed the requirement of one report to make its submission biennial, rather than annual. The Committee believes that elimination of these reports will help the Intelligence Community to allocate its resources properly towards areas of greatest congressional concern.

The Committee recognizes the concern expressed by the Intelligence Community about the impact of reporting requirements. The Committee suggests, for the fiscal year 2011 authorization act request, that the ODNI submit, even in advance of the Administration's formal requests for legislation, facts (including the cost of

preparing particular reports and the use of contract personnel, if any, to prepare reports) and proposals (including the consolidation of reports and lengthening the intervals between them) that will enable a fuller evaluation of alternatives for providing information to Congress. Also, for reports that by law are unclassified, the Committee requests that the ODNI advise the congressional intelligence committees about any system that is in place, or should be put in place, for their public dissemination.

#### Subtitle E—Other Matters

##### *Section 351. Extension of authority to delete information about receipt and disposition of foreign gifts and decorations*

Current law (5 U.S.C. 7342) requires that certain federal “employees”—a term that generally applies to all Intelligence Community officials and personnel and certain contract personnel, spouses, dependents, and others—file reports with their employing agency regarding receipt of gifts or decorations from foreign governments. Following compilation of these reports, the employing agency is required to file annually with the Secretary of State detailed information about the receipt of foreign gifts and decorations by its employees, including the source of the gift. The Secretary of State is required to publish a comprehensive list of the agency reports in the Federal Register.

With respect to Intelligence Community activities, public disclosure of gifts or decorations in the Federal Register has the potential to compromise intelligence sources (e.g., confirmation of an intelligence relationship with a foreign government) and could undermine national security. Recognizing this concern, the Director of Central Intelligence (DCI) was granted a limited exemption from reporting certain information about such foreign gifts or decorations where the publication of the information could adversely affect United States intelligence sources. Section 1079 of the Intelligence Reform Act extended a similar exemption to the DNI in addition to applying the existing exemption to the CIA Director.

Section 351 provides to the heads of each Intelligence Community element the same limited exemption from specified public reporting requirements that is currently authorized for the DNI and CIA Director. The national security concerns that prompt those exemptions apply equally to other Intelligence Community elements. Section 351 mandates that the information not provided to the Secretary of State be provided to the DNI, who is required to keep a record of such information, to ensure continued independent oversight of the receipt by Intelligence Community personnel of foreign gifts or decorations.

Gifts received in the course of ordinary contact between senior officials of elements of the Intelligence Community and their foreign counterparts should not be excluded under the provisions of Section 351 unless there is a serious concern that such contacts and gifts would adversely affect United States intelligence sources or methods.



*Section 352. Exemption of dissemination of terrorist identity information from Freedom of Information Act*

Section 352 provides an exemption for terrorist identity information disseminated for terrorist screening purposes from disclosure under the Freedom of Information Act (5 U.S.C. 552) in order to facilitate on an unclassified basis the sharing of those elements of information necessary for terrorist screening purposes.

*Section 353. Modification of availability of funds for different intelligence activities*

Section 353 conforms the text of Section 504(a)(3)(B) of the National Security Act of 1947 (50 U.S.C. 414(a)(3)(B) (governing the funding of intelligence activities)) with the text of Section 102A(d)(5)(A)(ii) of that Act (50 U.S.C. 403–1(d)(5)(A)(ii)), as amended by Section 1011(a) of the Intelligence Reform Act (governing the transfer and reprogramming by the DNI of certain intelligence funding).

The amendment replaces the “unforeseen requirements” standard in Section 504(a)(3)(B) with a more flexible standard to govern reprogrammings and transfers of funds authorized for a different intelligence or intelligence-related activity. Under the new standard, a reprogramming or transfer is authorized if, in addition to the other requirements of Section 504(a)(3), the new use of funds would “support an emergent need, improve program effectiveness, or increase efficiency.” This modification brings the standard for reprogrammings or transfers of intelligence funding into conformity with the standards applicable to reprogrammings and transfers under Section 102A of the National Security Act of 1947. The modification preserves congressional oversight of proposed reprogrammings and transfers while enhancing the Intelligence Community’s ability to carry out missions and functions vital to national security.

*Section 354. Limitation on reprogrammings and transfers of funds*

Section 354 modifies the reprogramming requirements set forth in Section 504 of the National Security Act of 1947 (50 U.S.C. 414) to provide in statute that, following a reprogramming notification from the DNI, Attorney General, or Secretary of Defense, appropriated funds may not be expended for a period of up to 90 days after a request for information about the reprogramming is made by one of the congressional intelligence committees. It also allows the President to authorize the reprogramming, regardless of the 90-day review period, to fulfill an urgent operational requirement (excluding cost overruns) when it is necessary for the Intelligence Community to carry out the reprogrammed activity prior to the completion of the review period set by the congressional intelligence committees.

Section 504 of the National Security Act of 1947 allows the Intelligence Community a certain degree of flexibility in reprogramming authorized and appropriated funds, as amended by Section 353, without having to seek additional legislation from Congress. Section 354 of the bill alters this delegation of authority to reprogram and transfer funds by formalizing a maximum time period for review by the congressional intelligence committees and instituting a

waiver mechanism to ensure that such review does not hamper urgent operational requirements.

*Section 355. Protection of certain national security information*

Section 355 amends Section 601 of the National Security Act of 1947 (50 U.S.C. 421) to increase the criminal penalties involving the disclosure of the identities of undercover intelligence officers and agents.

Section 355(a) amends Section 601(a) to increase criminal penalties for an individual with authorized access to classified information who intentionally discloses any information identifying a covert agent, if the individual knows that the United States is taking affirmative measures to conceal the covert agent's intelligence relationship to the United States. Currently, the maximum sentence for disclosure by someone who has had "authorized access to classified information that identifies a covert agent" is 10 years. Subsection (a)(1) of Section 345 of this Act increases that maximum sentence to 15 years.

Currently, under Section 601(b) of the National Security Act of 1947, the maximum sentence for disclosure by someone who "as a result of having authorized access to classified information, learns of the identity of a covert agent" is 5 years. Subsection (a)(2) of Section 355 of this Act increases that maximum sentence to 10 years.

Subsection (b) of Section 355 amends Section 603(a) of the National Security Act of 1947 (50 U.S.C. 423(a)) to provide that the annual report from the President on the protection of identities of certain United States undercover intelligence officers, agents, informants, and sources, also include an assessment of the need for any modification for the purpose of improving legal protections for covert agents.

*Section 356. National Intelligence Program budget request*

Section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53 (2007) (50 U.S.C. 415c), requires the DNI to disclose the aggregate amount of funds appropriated by Congress for the National Intelligence Program for each fiscal year beginning with fiscal year 2007. Section 601(b) provides that the President may waive or postpone such disclosure if certain conditions are met, beginning with fiscal year 2009.

Section 356 of the bill amends Section 601 of the Implementing Recommendations of the 9/11 Commission Act of 2007 to require that, on the date that the President submits to Congress the annual budget request, the President shall disclose to the public the aggregate amount of appropriations requested for that fiscal year for the National Intelligence Program. The section also eliminates the presidential waiver authority related to the public disclosure by the DNI of the aggregate amount of funds appropriated by Congress for the National Intelligence Program for any fiscal year.

*Section 357. Improving the review authority of the Public Interest Declassification Board*

Section 357 clarifies that the Public Interest Declassification Board may conduct reviews in response to requests from the committee of jurisdiction, or from individual members of the committee. This will, among other things, protect the opportunity of a

committee's minority to obtain the benefit of a Public Interest Declassification Board review. It also clarifies that the Board may consider the proper classification level of records, rather than simply consider whether or not they should be classified. This authority is important to address questions of excessive compartmentation or other over classification that may impede needed information sharing or impede adequate reviews within the Executive branch and oversight by the Congress.

*Section 358. Authority to designate undercover operations to collect foreign intelligence or counterintelligence*

Various provisions in the United States Code preclude the government from conducting the following activities: (1) the deposit of funds in a financial institution; (2) the lease or purchase of real property; (3) the establishment and operation of a proprietary business on a commercial basis; and (4) the utilization of proceeds of the operation to offset necessary and reasonable operational expenses. In recognition, however, of the important role such activities may play in the conduct of undercover operations, Public Law 102-395 (1992) (28 U.S.C. 533 note) provides a mechanism for the FBI to obtain an exemption from these otherwise applicable laws.

Under Public Law 102-395, an exemption may be obtained if the proposed activity is certified by the Director of the FBI and the Attorney General as being necessary to the conduct of the undercover operation. For national security investigations, the Director of the FBI may delegate certifying authority to an Assistant Director in the Counterterrorism, Counterintelligence, or Cyber Divisions at the FBI, and the Attorney General may delegate such authority to the Assistant Attorney General for the National Security Division at the Department of Justice.

Section 358 amends the current delegation level for both the FBI and the Department of Justice. It allows the FBI Director to delegate certifying authority to a level not lower than a Deputy Assistant Director in the National Security Branch. It also allows the Attorney General to delegate the certifying authority to a level not lower than a Deputy Assistant Attorney General in the National Security Division. It should be noted that this delegation level for the Department of Justice remains at a higher level than that which is currently required in criminal undercover operations.

The Committee is concerned that, because of both statutory and administrative limitations, the current delegation levels are insufficient to allow for timely processing of undercover exemptions. The success and safety of undercover operations can depend in part on the ability to do such simple tasks as open a bank account or rent an apartment for cover purposes in a timely manner. While the creation of the National Security Division at the Department of Justice has led to more efficient processing of some exemption requests, there remains room for improvement. The Committee believes that the new delegation levels established in Section 358 will encourage and facilitate further internal and administrative improvements in processing undercover exemptions both at the FBI and the Department of Justice, without sacrificing needed oversight within the FBI and Department of Justice.

*Section 359. Correcting long-standing material weaknesses*

Section 359 requires the heads of the five intelligence agencies that have been specifically required to produce auditable financial statements (the CIA, Defense Intelligence Agency (DIA), NGA, NRO, and NSA) to designate each senior management official who is responsible for correcting long-standing, correctable material weaknesses, and to notify the DNI and the congressional intelligence committees of these designations.

Under Section 359, the term “material weakness” has the meaning given that term under OMB Circular A–123, *Management’s Responsibility for Internal Control*, revised December 21, 2004. In particular, “[a] material weakness in internal controls is a reportable condition, or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected.”

The Committee has been dissatisfied with the lack of progress in correcting material weaknesses. Section 359 is intended to ensure there is clear accountability about who is responsible for correcting these deficiencies.

Section 359 pertains only to “long-standing” material weaknesses, defined as those that were identified in annual financial reports no later than fiscal year 2006. Also, Section 359 pertains only to material weaknesses that are correctable in the near term, i.e., those whose correction is not substantially dependent on a business information system that will not be fielded prior to fiscal year 2011. The head of an Intelligence Community agency head may be designated as the responsible official.

Section 359 also requires a senior intelligence management official to notify his agency head within five days of correcting a long-standing material weakness. The head of the agency then has 10 days to appoint an independent auditor who will determine whether the specified long-standing correctable material weakness has been corrected. If the correction is verified by the independent audit, the agency head shall notify the congressional intelligence committees that the material weakness has been corrected.

The Committee believes that this legislative step is necessary to establish clear accountability for correcting these long-standing correctable material weaknesses. The Committee expects the DNI and Intelligence Community agency heads to consider progress towards correcting these material weaknesses to be an important consideration in determining any awards, bonuses, or promotions for these designated senior officials.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE  
INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

*Section 401. Accountability reviews by the Director of National Intelligence*

Section 401 provides that the DNI shall have new authority to conduct accountability reviews of elements within the Intelligence Community and the personnel of those elements. The primary innovation of this provision is the authority to conduct accountability

reviews concerning an entire element of the Intelligence Community in relation to failures or deficiencies.

This accountability process is intended to be separate and distinct from any accountability reviews being conducted internally by the elements of the Intelligence Community or their Inspectors General, and is not intended to limit the authorities of the DNI with respect to his supervision of the CIA.

Section 401 requires that the DNI, in consultation with the Attorney General, formulate guidelines and procedures that will govern accountability reviews. The Committee envisions that these guidelines will govern the process by which the DNI can collect sufficient information from the Intelligence Community to assess accountability for a given incident.

Any findings and recommendations for corrective or punitive action made by the DNI shall be provided to the head of the applicable element of the Intelligence Community. If the head of such element does not implement the recommendations, then the congressional intelligence committees must be notified and provided the reasons for the determination by the head of the element.

In addition, to avoid a construction that a committee of Congress on its own could require such a review over the objection of the DNI, a concern raised by the ODNI, the section makes clear that the DNI shall conduct a review if the DNI determines it is necessary, and the DNI may conduct an accountability review (but is not statutorily required to do so) if requested by one of the congressional intelligence committees.

This enhancement to the authority of the DNI is warranted given the apparent reluctance of various elements of the Intelligence Community to hold their agencies or personnel accountable for significant failures or deficiencies. Recent history provides several examples of serious failures to adhere to sound analytic tradecraft. In its reviews of both the September 11, 2001 terrorist attacks and the faulty Iraq prewar assessments on weapons of mass destruction, the Committee found specific examples of these failures yet no one within the Intelligence Community has been held accountable. Other examples of a lack of accountability within the Intelligence Community can be found by examining the history of certain major system acquisition programs. Despite clear management failures that resulted in significant cost overruns and unreasonable scheduling delays, these programs continued to stumble along without any imposition of accountability.

The Committee hopes that this modest increase in the DNI's authorities will encourage elements within the Intelligence Community to put their houses in order by imposing accountability for significant failures and deficiencies. Section 401 will enable the DNI to get involved in the accountability process in the event that an element of the Intelligence Community cannot or will not take appropriate action.

#### *Section 402. Authorities for intelligence information sharing*

Section 402 amends Section 102A(g)(1) of the National Security Act of 1947 (50 U.S.C. 403-1(g)(1)) to provide the DNI statutory authority to use National Intelligence Program funds to quickly address deficiencies or needs that arise in intelligence information access or sharing capabilities.

The new Section 102A(g)(1)(G) authorizes the DNI to provide to a receiving agency or component, and for that agency or component to accept and use, funds or systems (which would include services or equipment) related to the collection, processing, analysis, exploitation, and dissemination of intelligence information.

The new Section 102A(g)(1)(H) grants the DNI authority to provide funds to non-National Intelligence Program activities for the purpose of addressing critical gaps in intelligence information access or sharing capabilities. Without this authority, development and implementation of necessary capabilities could be delayed by an agency's lack of authority to accept or utilize systems funded from the National Intelligence Program, inability to use or identify current-year funding, or concerns regarding the augmentation of appropriations.

These are similar to authorities granted to the NGA for developing and fielding systems of common concern relating to imagery intelligence and geospatial intelligence. See Section 105(b)(2)(D)(ii) of the National Security Act of 1947 (50 U.S.C. 403–5). Section 402 also requires the DNI to submit a report to the congressional intelligence committees by February 1st annually from fiscal year 2010 through fiscal year 2013 providing details on how this authority has been exercised during the preceding fiscal year.

*Section 403. Authorities for interagency funding*

The DNI should be able to rapidly focus the Intelligence Community on an intelligence issue through a coordinated effort that uses all available resources. The ability to coordinate the Intelligence Community response to an emerging threat should not depend on the budget cycle and should not be constrained by general limitations in appropriations law (e.g., 31 U.S.C. 1346) or other prohibitions on interagency financing of boards, commissions, councils, committees, or similar groups.

To provide this flexibility, Section 403 grants the DNI the authority to approve interagency financing of national intelligence centers established under Section 119B of the National Security Act of 1947 (50 U.S.C. 404o–2). The section also authorizes interagency funding for boards, commissions, councils, committees, or similar groups established by the DNI for a period not to exceed two years. This would include the interagency funding of Intelligence Community mission managers. Under Section 402, the DNI could authorize the pooling of resources from various Intelligence Community agencies to finance national intelligence centers or other organizational groupings designed to address identified intelligence matters. The provision also expressly permits Intelligence Community elements, upon the request of the DNI, to fund or participate in these interagency activities. The DNI is limited in his use of this authority to appropriated funds.

Under Section 403, the DNI is to submit a report to the congressional intelligence committees by February 1st annually from fiscal year 2011 through fiscal year 2014 providing details on how this authority has been exercised during the preceding fiscal year.

*Section 404. Location of the Office of the Director of National Intelligence*

Section 404 addresses the issue of the location of the Office of the DNI. Section 404 repeals the ban on the co-location of the Office of the DNI with any other Intelligence Community element, which was to take effect on October 1, 2008, by replacing that provision of the National Security Act of 1947 (50 U.S.C. 403–3) with a new subsection 103(e) that allows the ODNI to be located outside the District of Columbia within the Washington Metropolitan Region.

In his 2008 legislative request for the fiscal year 2009 authorization, the DNI asked, for the first time, that Congress provide that “[t]he headquarters of the Office of the Director of National Intelligence may be located in the District of Columbia or elsewhere in the Metropolitan Region, as that term is defined in Section 8301 of title 40, United States Code.” The purpose of this section is to provide statutory authorization for the location of the ODNI outside of the District of Columbia.

Section 72 of Title 4, United States Code—a codification enacted in 1947 which derived from a statute signed into law by President George Washington in 1790—requires that “[a]ll offices attached to the seat of government shall be exercised in the District of Columbia and not elsewhere, except as otherwise expressly provided by law.” In 1955, just eight years after the 1947 codification, Congress granted statutory authority for the Director of Central Intelligence to provide for a headquarters of the Central Intelligence Agency either in the District of Columbia “or elsewhere.” 69 Stat. 324, 349.

Pursuant to the Committee’s direction during consideration of the fiscal year 2009 authorization act, the ODNI requested guidance from the Department of Justice’s Office of Legal Counsel (OLC) about the need for a statute authorizing the location of the ODNI outside the District of Columbia. The ODNI has informed the Committee that OLC has informally advised the ODNI that there is no basis to exclude the ODNI from the requirement of 4 U.S.C. 72 and that a specific exception is needed to authorize the location of the ODNI headquarters outside the District of Columbia. The Committee urges the ODNI to continue to study, and report to the congressional intelligence committees, about the impact if any of the ODNI’s current location outside of the District of Columbia on the daily implementation of the ODNI’s responsibilities with respect to the President, the Congress, and the elements of the Intelligence Community.

*Section 405. Additional duties of the Director of Science and Technology*

Section 405 clarifies the duties of the Director of Science and Technology (DS&T) and the Director of the National Intelligence Science and Technology Committee (NISTC). The Committee expects the DS&T to systematically identify, assess, and prioritize the most significant intelligence challenges that require technical solutions, set long-term science and technology goals, develop a strategy/roadmap to be shared with the congressional intelligence committees that meets these goals, and prioritize and coordinate efforts across the Intelligence Community. As chair of the NISTC, the DS&T should leverage the expertise of the committee to accomplish these duties. Section 405(b) is a Sense of the Congress that

the DS&T should report only to a member of the ODNI who is appointed by the President and confirmed by the Senate.

*Section 406. Title and appointment of Chief Information Officer of the Intelligence Community*

Section 406 expressly designates the position of Chief Information Officer in the Office of the Director of National Intelligence as Chief Information Officer of the Intelligence Community (IC CIO). The modification to this title is consistent with the position's overall responsibilities as outlined in Section 103G of the National Security Act of 1947 (50 U.S.C. 403-3g). Section 406 also eliminates the requirement that the IC CIO be confirmed by the Senate while retaining the requirement that the IC CIO be appointed by the President. The continued requirement of presidential appointment emphasizes that the IC CIO has important responsibilities for the Intelligence Community enterprise architecture with respect to the whole of the Intelligence Community.

*Section 407. Inspector General of the Intelligence Community*

Section 1078 of the Intelligence Reform Act authorizes the DNI to establish an Office of Inspector General if the DNI determines that an Inspector General (IG) would be beneficial to improving the operations and effectiveness of the ODNI. It further provides that the DNI may grant to the IG any of the duties, responsibilities, and authorities set forth in the Inspector General Act of 1978. The DNI has appointed an IG and has granted certain authorities pursuant to DNI Instruction No. 2005-10 (September 7, 2005).

As this Committee urged in reports on proposed authorization acts for fiscal years 2006 through 2009, a strong IG is vital to achieving the goal, set forth in the Intelligence Reform Act, of improving the operations and effectiveness of the Intelligence Community. It is also vital to achieving the broader goal of identifying problems and deficiencies, wherever they may be found in the Intelligence Community, with respect to matters within the responsibility and authority of the DNI, including the manner in which elements of the Intelligence Community interact with each other in providing access to information and undertaking joint or cooperative activities. By way of a new Section 103H of the National Security Act of 1947, Section 407 of this Act establishes an Inspector General of the Intelligence Community in order to provide to the DNI, and, through reports, to the Congress, the benefits of an IG with full statutory authorities and the requisite independence.

The Office of the IG is to be established within the ODNI. The Office of the IG created by this bill is to replace and not duplicate the current Office of the IG for the ODNI. The IG will keep both the DNI and the congressional intelligence committees fully and currently informed about problems and deficiencies in Intelligence Community programs and operations and the need for corrective actions. The IG will be appointed by the President, with the advice and consent of the Senate, and will report directly to the DNI. To bolster the IG's independence within the Intelligence Community, the IG may be removed only by the President, who must communicate the reasons for the removal to the congressional intelligence committees.



Under the new subsection 103H(e), the DNI may prohibit the IG from conducting an investigation, inspection, audit, or review if the DNI determines that is necessary to protect vital national security interests. If the DNI exercises this authority, the DNI must provide the reasons to the congressional intelligence committees within seven days. The IG may submit comments in response to the congressional intelligence committees.

The IG will have direct and prompt access to the DNI and any Intelligence Community employee, or employee of a contractor, whose testimony is needed. The IG will also have direct access to all records that relate to programs and activities for which the IG has responsibility. Failure to cooperate will be grounds for appropriate administrative action.

The IG will have subpoena authority. However, information within the possession of the United States Government must be obtained through other procedures. Subject to the DNI's concurrence, the IG may request information from any United States Government department, agency, or element. They must provide the information to the IG insofar as is practicable and not in violation of law or regulation.

The IG must submit semiannual reports to the DNI that include a description of significant problems relating to Intelligence Community programs and activities within the responsibility and authority of the DNI. Portions of the reports involving a component of a department of the United States Government are to be provided to the head of the department at the same time the report is provided to the DNI. The reports must include a description of IG recommendations and a statement whether corrective action has been completed. Within 30 days of receiving each semiannual report from the IG, the DNI must submit it to Congress.

The IG must immediately report to the DNI particularly serious or flagrant problems, abuses, or deficiencies. Within seven days, the DNI must transmit those reports to the intelligence committees together with any comments. In the event the IG is unable to resolve any differences with the DNI affecting the duties or responsibilities of the IG or the IG conducts an investigation, inspection, audit or review that focuses on certain high-ranking officials, the IG is authorized to report directly to the congressional intelligence committees.

Intelligence Community employees, or employees of contractors, who intend to report to Congress an "urgent concern"—such as a violation of law or Executive order, a false statement to Congress, or a willful withholding from Congress—may report such complaints and supporting information to the IG. Following a review by the IG to determine the credibility of the complaint or information, the IG must transmit such complaint and information to the DNI. On receiving the complaints or information from the IG (together with the IG's credibility determination), the DNI must transmit the complaint or information to the intelligence committees. If the IG finds a complaint or information not to be credible, the reporting individual may still submit the matter directly to the committees by following appropriate security practices outlined by the DNI. Reprisals or threats of reprisal against reporting individuals constitute reportable "urgent concerns." The Committee will not tolerate actions by the DNI, or by any Intelligence Community

element, constituting a reprisal for reporting an “urgent concern” or any other matter to Congress. Nonetheless, reporting individuals should ensure that the complaint and supporting information are provided to Congress consistent with appropriate procedures designed to protect intelligence sources and methods and other sensitive matters.

For matters within the jurisdiction of both the IG of the Intelligence Community and an IG for another Intelligence Community element (or for a parent department or agency), the Inspectors General shall expeditiously resolve who will undertake the investigation, inspection, audit, or review. In attempting to resolve that question, the Inspectors General may request the assistance of the Intelligence Community Inspectors General Forum (a presently functioning body whose existence is ratified by Section 407). In the event that the Inspectors General are still unable to resolve the question, they shall submit it to the DNI and the head of the agency or department for resolution.

An IG for an Intelligence Community element must share the results of any investigation, inspection, audit, or evaluation with any other IG, including the Inspector General of the Intelligence Community, who otherwise would have had jurisdiction over the investigation, inspection, audit, or evaluation.

Consistent with existing law, the Inspector General must report to the Attorney General any information, allegation, or complaint received by the Inspector General relating to violations of Federal criminal law.

Section 407 also provides for the transition from the Office of the IG of the ODNI to the Office of the IG of the Intelligence Community.

Following the Committee’s last report in May 2008 of a provision establishing an IG of the Intelligence Community, Congress enacted the Inspector General Reform Act of 2008, Public Law 110–409. In light of this recent determination by the Congress to protect and augment the authority of Inspectors General throughout the Government, the Committee has provided for conforming changes in the IG provision it is now reporting. Among these provisions is authority for the IG to appoint a counsel. Section 407 makes clear that it is not to be construed to alter the duties and responsibilities of the General Counsel of the Office of the Director of National Intelligence.

#### *Section 408. Chief Financial Officer of the Intelligence Community*

Section 408 amends Title I of the National Security Act of 1947 (50 U.S.C. 402 et seq.) to establish in statute a Chief Financial Officer of the Intelligence Community (IC CFO) to assist the DNI in carrying out budgetary, acquisition, and financial management responsibilities.

By way of a new Section 103I of the National Security Act of 1947, under Section 408, the IC CFO will, to the extent applicable, have the duties, responsibilities, and authorities specified in the Chief Financial Officers Act of 1990. The IC CFO will serve as the principal advisor to the DNI and the Principal Deputy DNI on the management and allocation of Intelligence Community budgetary resources, and shall establish and oversee a comprehensive and integrated strategic process for resource management within the In-

telligence Community. Section 408 charges the IC CFO with ensuring that the strategic plan and architectures of the DNI are based on budgetary constraints as specified in the future budget projections required in Section 325.

Section 408 also charges the IC CFO with ensuring that major system acquisitions satisfy validated national requirements for meeting the DNI's strategic plans and that such requirements are prioritized based on budgetary constraints as specified in the future budget projections required in Section 325. To guarantee this is achieved in practice, under Section 408, prior to obligation or expenditure of funds for major system acquisitions to proceed to Milestone A (development) or Milestone B (production), requirements must be validated and prioritized based on budgetary constraints as specified in Section 325.

Section 408 requires that the IC CFO preside, or assist in presiding, over any mission requirement, architectural, or acquisition board formed by the ODNI, and to coordinate and approve representations to Congress by the Intelligence Community regarding National Intelligence Program budgetary resources. An individual serving as the IC CFO may not at the same time also serve as a CFO of any other department or agency.

*Section 409. Leadership and location of certain offices and officials*

Section 409 confirms in statute that various offices are within the ODNI: (1) the Chief Information Officer of the Intelligence Community; (2) the Inspector General of the Intelligence Community; (3) the Director of the National Counterterrorism Center (NCTC); (4) the Director of the National Counter Proliferation Center (NCPC); and (5) the Chief Financial Officer of the Intelligence Community. It also expressly provides in statute that the DNI shall appoint the Director of the NCPC, which is what has been done by administrative delegation from the President.

*Section 410. National Space Intelligence Office*

Section 410 establishes a National Space Intelligence Office (NSIO) within the ODNI to facilitate a better understanding of future threats to U.S. space assets, as well as potential threats to the United States from space. It is not the intent of the Committee that the NSIO be a physical consolidation of existing intelligence entities with responsibilities for various types of intelligence related to space. Rather, the functions of the NSIO, among others delineated in Section 410, will be to coordinate and provide policy direction for the management of space-related intelligence assets as well as to prioritize collection activities consistent with the DNI's National Intelligence Collection Priorities.

The NSIO is to augment the existing efforts of the National Air and Space Intelligence Center (NASIC) and Missile and Space Intelligence Center (MSIC); it is not designed to replace them. The Committee intends that NSIO work closely with NASIC and MSIC to ensure a coordinated Intelligence Community response to issues that intersect the responsibilities of all three organizations.

The NSIO Director shall be the National Intelligence Officer for Science and Technology. The Committee encourages appointment of an Executive Director from the Senior Intelligence Service.

*Section 411. Operational files in the Office of the Director of National Intelligence*

In the CIA Information Act (Public Law 98–477 (1984) (50 U.S.C. 431 et seq.)), Congress authorized the DCI to exempt operational files of the CIA from several requirements of the Freedom of Information Act (FOIA), particularly those requiring search and review in response to FOIA requests. In a series of amendments to Title VII of the National Security Act of 1947, Congress has extended the exemption to the operational files of the NGA, the NSA, the NRO, and the DIA. It has also provided that files of the Office of the National Counterintelligence Executive (NCIX) should be treated as operational files of the CIA (to the extent they meet the criteria for CIA operational files).

Section 411 adds a new Section 706 to the National Security Act of 1947. Components of the ODNI, including the NCTC, require access to information contained in CIA and other operational files. The purpose of Section 411 is to make clear that the operational files of any Intelligence Community component, for which an operational files exemption is applicable, retain their exemption from FOIA search, review, disclosure, or publication. They also retain their exemption when they are incorporated in any substantially similar files of the ODNI.

Section 411 provides several limitations. The exemption does not apply to information disseminated beyond the ODNI. Also, as Congress has provided in the operational files exemptions for the CIA and other Intelligence Community elements, Section 411 provides that the exemption from search and review does not apply to requests by United States citizens or permanent residents for information about themselves (although other FOIA exemptions, such as appropriate classification, may continue to protect such files from public disclosure). The search and review exemption would not apply to the subject matter of congressional or Executive branch investigations into improprieties or violations of law.

Section 411 also provides for a decennial review by the DNI to determine whether exemptions may be removed from any category of exempted files. It provides that this review shall include consideration of the historical value or other public interest in the subject matter of those categories and the potential for declassifying a significant part of the information contained in them. The Committee underscores the importance of this requirement, which applies to the other operational exemptions in Title VII.

The Committee also reiterates its interest in being advised by the DNI about the benefits of coordinating all the decennial reviews required by Title VII. Specifically, the Committee requests the DNI, through the Chief Information Officer of the Intelligence Community, to consider, and advise the congressional intelligence committees about, conducting the next review in each covered Intelligence Community element during Fiscal Year 2010 so that the next review for every element covered by an operational files exemption under Title VII, and the following decennial reviews, are conducted in an integrated manner in accordance with consistent standards developed under guidance established by the Chief Information Officer. The committees should be informed about the design, conduct, and results of these reviews, which should include

the administrative and judicial experience of the various elements of the Intelligence Community under operational file exemptions.

*Section 412. Counterintelligence initiatives for the Intelligence Community*

Section 412 amends Section 1102(a) of the National Security Act of 1947 (50 U.S.C. 442a) to eliminate the requirement that the NCIX perform certain security functions more appropriately carried out by other components of the Intelligence Community.

*Section 413. Applicability of the Privacy Act to the Director of National Intelligence and the Office of the Director of National Intelligence*

The Privacy Act (5 U.S.C. 552a) has long contained a provision under which the DCI and then (after enactment of the Intelligence Reform Act) the CIA Director could promulgate rules to exempt any system of records within the CIA from certain disclosure requirements under the Act. The provision was designed to ensure that the CIA could provide safeguards for certain sensitive information in its records systems. In assuming the leadership of the Intelligence Community, the DNI similarly requires the ability to safeguard sensitive information in records systems within the ODNI. Section 413 extends to the DNI the authority to promulgate rules under which records systems of the ODNI may be exempted from certain Privacy Act disclosure requirements.

*Section 414. Inapplicability of Federal Advisory Committee Act to advisory committees of the Office of the Director of National Intelligence*

Congress enacted the Federal Advisory Committee Act (FACA) (5 U.S.C. App.) to regulate the use of advisory committees throughout the Federal Government. FACA sets forth the responsibilities of the Executive branch with regard to such committees and outlines procedures and requirements for them. As originally enacted in 1972, FACA expressly exempted advisory committees utilized by the CIA and the Federal Reserve System. Section 414 amends FACA to extend this exemption, for the same policy reasons underlying the original CIA exemption, to advisory committees established or used by the ODNI. Section 414 requires the DNI and the Director of the CIA to inform the intelligence committees on a yearly basis about the composition and use by the ODNI and the CIA of advisory committees.

*Section 415. Membership of the Director of National Intelligence on the Transportation Security Oversight Board*

Section 415 substitutes the DNI, or the DNI's designee, as a member of the Transportation Security Oversight Board established under Section 115(b)(1) of Title 49, United States Code, in place of the CIA Director or CIA Director's designee.

*Section 416. Repeal of certain authorities relating to the Office of the National Counterintelligence Executive*

Section 416 amends the authorities and structure of the Office of the NCIX to eliminate certain independent administrative authorities that had been vested in the NCIX when that official was ap-

pointed by and reported to the President. Those authorities are unnecessary now that the NCIX is to be appointed by and is under the authority of the DNI.

*Section 417. Misuse of the Office of the Director of National Intelligence name, initials, or seal*

Section 417 prohibits the unauthorized use of the official name, initials or seal of the ODNI. Section 417 also permits the Attorney General to pursue injunctive relief for such unauthorized use. The provision is modeled on section 13 of the CIA Act of 1949 (50 U.S.C. 403(m)) which provides similar protection against misuse of the name, initials, or seal of the CIA.

Subtitle B—Central Intelligence Agency

*Section 421. Additional functions and authorities for protective personnel of the Central Intelligence Agency*

Section 421 amends Section 5(a)(4) of the CIA Act of 1949 (50 U.S.C. 403f(a)(4)) which authorizes protective functions by designated security personnel who serve on CIA protective details. Section 421 authorizes the CIA Director on the request of the DNI to make CIA protective detail personnel available to the DNI and to other personnel within the ODNI.

*Section 422. Appeals from decisions involving contracts of the Central Intelligence Agency*

Section 422 amends Section 8(d) of the Contract Disputes Act of 1978 (41 U.S.C. 607(d)) to provide that an appeal from a dispute arising out of a CIA contract shall be filed with whichever of the Armed Services Board of Contract Appeals or the Civilian Board of Contract Appeals is specified in the contract and that such board shall have jurisdiction to decide the appeal.

*Section 423. Deputy Director of the Central Intelligence Agency*

Section 423 provides for a Deputy Director of the CIA in a new Section 104B of the National Security Act of 1947 (50 U.S.C. 402 et seq.). Under the new Section 104B, the Deputy Director of the CIA shall be appointed by the President and confirmed by the Senate, shall assist the Director of the CIA in carrying out the Director's duties and responsibilities, and shall assume those duties and responsibilities in the event of the Director's absence, disability, or when the position is vacant.

Prior to the Intelligence Reform Act, Congress had provided by law for the appointment by the President, with Senate confirmation, of a Deputy Director of Central Intelligence. The Intelligence Reform Act abolished that position and was silent on any deputy to the Director of the CIA. Since enactment of the Intelligence Reform Act, the position of Deputy Director at the CIA has been solely a product of administrative action.

Given the sensitive nature of the CIA's operations, the position of Deputy Director as well as that of the position of the Director merit consideration through the process of presidential appointment and Senate confirmation. That process also ensures that in the event of a vacancy in the position of Director, or during the absence or disability of the Director, Congress will have previously

expressed its confidence in the ability of the Deputy Director to assume those additional duties.

Section 423(c) provides that the amendments made by Section 423 apply prospectively. Therefore, the Deputy Director of the CIA on the date of enactment will not be affected by the amendments.

*Section 424. Authority to authorize travel on a common carrier*

Section 424 amends Section 116(b) of the National Security Act of 1947 (50 U.S.C. 404k(b)). Section 116(b) of the National Security Act of 1947 allows the DNI to authorize travel on common carriers for certain intelligence collection personnel, and it further allows the DNI to delegate this authority to the Principal Deputy Director of National Intelligence or to the Director the Central Intelligence Agency. This provision permits the Director of the CIA to re-delegate this authority within the Central Intelligence Agency.

*Section 425. Inspector General of the Central Intelligence Agency*

Section 425 amends Section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q(b)) which established a statutory CIA Inspector General. The amendment updates and clarifies the statute in light of revisions made by Congress in the Inspector General Reform Act of 2008 (Public Law 110–409) and the recommendations in the most recent semiannual report of the CIA IG. Among other provisions, Section 425 expands the protections against reprisals that now apply to CIA employees who bring complaints to the CIA IG to any CIA employee who provides information to the CIA IG. Section 425 provides that the CIA IG has final approval of the selection of internal and external candidates for employment with the Office of the IG and may appoint a counsel who reports to the IG. Section 425 provides that this is not to be construed to alter the duties and responsibilities of the General Counsel of the CIA.

*Section 426. Budget of the Inspector General of the Central Intelligence Agency*

Section 426 further amends Section 17 of the CIA Act to require the DNI to provide to the President the budget amount requested by the CIA IG and to provide that information to the congressional appropriations and intelligence committees, together with any comments of the CIA IG.

*Section 427. Public availability of unclassified versions of certain intelligence products*

Section 427 requires the Director of the Central Intelligence Agency to make public unclassified versions of four documents which assess the information gained from the interrogation of high-value detainees. One of the documents is a memorandum and the other three are finished intelligence products. The unclassified versions of these documents will permit the American people to make their own determination of the value of the material included in these documents.

## Subtitle C—Defense Intelligence Components

*Section 431. Inspector General matters*

The Inspector General Act of 1978 (5 U.S.C. App.) establishes a government-wide system of Inspectors General, some appointed by the President with the advice and consent of the Senate and others “administratively appointed” by the heads of their respective Federal entities. These IGs are authorized to “conduct and supervise audits and investigations relating to the programs and operations” of the government and “to promote economy, efficiency, and effectiveness in the administration of, and . . . to prevent and detect fraud and abuse in, such programs and operations.” 5 U.S.C. App. 2. They also perform an important reporting function, “keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of . . . programs and operations and the necessity for and progress of corrective action.” *Id.* The investigative authorities exercised by Inspectors General, and their relative independence from the government operations they audit and investigate, provide an important mechanism to ensure that the operations of the government are conducted as efficiently and effectively as possible.

The IGs of the CIA and Departments of Defense, Energy, Homeland Security, Justice, State, and Treasury are appointed by the President with the advice and consent of the Senate. These IGs—authorized by either the Inspectors General Act of 1978 or Section 17 of the CIA Act—enjoy a degree of independence from all but the head of their respective departments or agencies. They also have explicit statutory authority to access information from their departments or agencies or other United States Government departments and agencies and may use subpoenas to access information (e.g., from an agency contractor) necessary to carry out their authorized functions.

The NRO, DIA, NSA and NGA have established their own “administrative” Inspectors General. However, because they are not identified in Section 8G of the Inspector General Act of 1978, they lack explicit statutory authorization to access information relevant to their audits or investigations, or to compel the production of information via subpoena. This lack of authority could impede access to information, in particular information from contractors that is necessary for them to perform their important function. These Inspectors General also lack the indicia of independence necessary for the Government Accountability Office to recognize their annual financial statement audits as being in compliance with the Chief Financial Officers Act of 1990 (Public Law 101–576). The lack of independence also prevents the DoD IG, and would prevent the Inspector General of the Intelligence Community, from relying on the results of NRO, DIA, NSA, or NGA Inspector General audits or investigations when such audits must meet “generally accepted government auditing standards.”

To provide an additional level of independence and to ensure prompt access to the information necessary for these IGs to perform their audits and investigations, Section 431 amends Section 8G(a)(2) of the Inspector General Act of 1978 to include the NRO, DIA, NSA, and NGA as “designated federal entities.” As so designated, the heads of these Intelligence Community elements will



be required by statute to administratively appoint Inspectors General for these agencies.

Also, as designated Inspectors General under the Inspector General Act of 1978, these Inspectors General will be responsible to the heads of the NRO, DIA, NSA, and NGA. The removal or transfer of any of these Inspectors General by the head of their office or agency must be promptly reported to the congressional intelligence committees. These Inspectors General will also be able to exercise other investigative authorities, including those governing access to information and the issuance of subpoenas, utilized by other Inspectors General under the Inspector General Act of 1978.

To protect vital national security interests, Section 431 permits the Secretary of Defense, in consultation with the DNI, to prohibit the Inspectors General of the NRO, DIA, NSA, and NGA from initiating, carrying out, or completing any audit or investigation they are otherwise authorized to conduct. This authority is similar to the authority of the CIA Director under Section 17 of the CIA Act with respect to the Inspector General of the CIA and the authority of the Secretary of Defense under Section 8 of the Inspector General Act of 1978 with respect to the DoD Inspector General. It will provide the Secretary of Defense, in consultation with the DNI, a mechanism to protect extremely sensitive intelligence sources and methods or other vital national security interests. The Committee expects that this authority will be exercised rarely by the DNI or the Secretary of Defense.

*Section 432. Confirmation of appointment of heads of certain components of the Intelligence Community*

Under present law and practice, the Directors of the NSA, NGA, and NRO, each with a distinct and significant role in the national intelligence mission, are not confirmed by the Senate in relation to their leadership of these agencies. Presently, the President appoints the Directors of NSA and NGA, and the Secretary of Defense appoints the Director of the NRO. None of the appointments must be confirmed by the Senate, unless a military officer is promoted or transferred into the position. Under that circumstance, Senate confirmation of the promotion or assignment is the responsibility of the Committee on Armed Services. That committee's review, however, relates to the military promotion or assignment and not specifically to the assumption by the individual of the leadership of a critical Intelligence Community element.

Section 432 provides, expressly and uniformly, that the heads of each of these entities shall be nominated by the President and that the nominations will be confirmed by the Senate. The NSA, NGA, and NRO play a critical role in the national intelligence mission. Their spending comprises a significant portion of the entire intelligence budget of the United States, and a substantial portion of the National Intelligence Program. Through advice and consent, the Senate can enable the Congress to fulfill more completely its responsibility for providing oversight to the intelligence activities of the United States Government. Section 432 does not alter the role of the Committee on Armed Services in reviewing and approving the promotion or assignment of military officers.

Section 432(e) provides that the amendments made by Section 432 apply prospectively. Therefore, the Directors of the NSA, NGA,

and NRO on the date of the enactment of this Act will not be affected by the amendments, which will apply initially to the appointment and confirmation of their successors.

The Committee undertakes to work with the Committee on Armed Services, as it has done and will do with any other committee that has jurisdiction over the Executive branch department of an Intelligence Community element, to provide for an appropriate manner of proceeding that recognizes the interests of both committees and ultimately the Senate in an efficient and thorough nomination process.

*Section 433. Clarification of national security missions of National Geospatial-Intelligence Agency for analysis and dissemination of certain intelligence information*

The National Imagery and Mapping Agency Act of 1996 (Public Law 104–201 (1996) (NIMA Act)) formally merged the imagery analysis and mapping efforts of the Department of Defense and the CIA. In the NIMA Act, Congress cited a need “to provide a single agency focus for the growing number and diverse types of customers for imagery and geospatial information resources within the Government . . . to harness, leverage, and focus rapid technological developments to serve the imagery, imagery intelligence, and geospatial information customers.” Section 1102(1) of the NIMA Act. Since then, there have been rapid developments in airborne and commercial imagery platforms, new imagery and geospatial phenomenology, full motion video, and geospatial analysis tools.

Section 921 of the National Defense Authorization Act for Fiscal Year 2004 (Public Law 108–136 (2003)) changed the name of the National Imagery and Mapping Agency to the National Geospatial-Intelligence Agency. The name change was intended to introduce the term “geospatial intelligence” to better describe the unified activities of NGA related to the “analysis and visual representation of characteristics of the earth and activity on its surface.” See S. Rep. 108–46 (2003) (accompanying The National Defense Authorization Act for Fiscal Year 2004, S. 1050, 108th Cong., 1st Sess.).

Though the NGA has made significant progress toward unifying the traditional imagery analysis and mapping missions of the CIA and Department of Defense, it has been slow to embrace other facets of “geospatial intelligence,” including the processing, storage, and dissemination of full motion video (FMV) and ground-based photography. Rather, the NGA’s geospatial products repositories—containing predominantly overhead imagery and mapping products—continue to reflect its heritage. While the NGA is belatedly beginning to incorporate more airborne and commercial imagery, its data holdings and products are nearly devoid of FMV and ground-based photography.

The Committee believes that FMV and ground-based photography should be included, with available positional data, in NGA data repositories for retrieval on Department of Defense and Intelligence Community networks. Current mission planners and military personnel are well-served with traditional imagery products and maps, but FMV of the route to and from a facility or photographs of what a facility would look like to a foot soldier—rather than from an aircraft—would be of immense value to military per-

sonnel and intelligence officers. Ground-based photography is amply available from open sources, as well as other government sources such as military units, United States embassy personnel, Defense Attachés, Special Operations Forces, foreign allies, and clandestine officers. These products should be better incorporated into NGA data holdings.

To address these concerns, Section 433 adds an additional national security mission to the responsibilities of the NGA. To fulfill this new mission, NGA would be required, as directed by the DNI, to develop a system to facilitate the analysis, dissemination, and incorporation of likenesses, videos, or presentations produced by ground-based platforms, including handheld or clandestine photography taken by or on behalf of human intelligence collection organizations or available as open-source information into the national system for geospatial intelligence.

Section 433 also makes clear that this new responsibility does not include the authority to manage the tasking of handheld or clandestine photography taken by or on behalf of human intelligence collection organizations. Although Section 433 does not give the NGA direct authority to set technical requirements for collection of handheld or clandestine photography, the Committee encourages the NGA to engage Intelligence Community partners on these technical requirements to ensure that their output can be incorporated into the National System for Geospatial-Intelligence.

Section 433 does not modify the definition of “imagery” found in Section 467(2)(A) of Title 10 of the United States Code, or alter any of the existing national security missions of the NGA. With Section 433, the Committee stresses the merits of FMV and ground-based photography and clarifies that the exclusion of “handheld or clandestine photography taken by or on behalf of human intelligence organizations” from the definition of “imagery” under the NIMA Act does not prevent the exploitation, dissemination, and archiving of that photography. In other words, NGA would still not dictate how human intelligence agencies collect such ground-based photography, have authority to modify its classification or dissemination limitations, or manage the collection requirements for such photography. Rather, NGA should simply avail itself of this ground-based photography, regardless of the source, but within the security handling guidelines consistent with the photography’s classification as determined by the appropriate authority.

*Section 434. Defense Intelligence Agency counterintelligence and expenditures*

Section 434 amends Section 105 of the National Security Act of 1947, on the responsibilities of Intelligence Community elements in the Department of Defense, to make clear that the responsibilities of the DIA include counterintelligence as well as human intelligence activities. Section 434 also provides authority for the Director of the DIA to account for expenditures for human intelligence and counterintelligence in a manner, similar to that available to the CIA, which does not disclose human sources. The amendment requires that the DIA Director shall report annually to the congressional intelligence committees on the use of that expenditure authority. It is the intention of the Committee that the DIA Director shall carefully monitor the use of this authority to ensure that the

flexibility it permits is used only in furtherance of the counterintelligence and human intelligence responsibilities of the DIA.

#### Subtitle D—Other Elements

##### *Section 441. Codification of additional elements of the intelligence community*

Section 441 restores, with respect to the United States Coast Guard, the prior definition of “intelligence community” in the National Security Act of 1947 applicable to that service. *See* 50 U.S.C. 401a. Section 1073 of the Intelligence Reform Act modified the definition of “intelligence community,” inadvertently limiting the Coast Guard’s inclusion in the Intelligence Community to the Office of Intelligence or those portions of the Coast Guard concerned with the analysis of intelligence. Section 441 clarifies that all of the Coast Guard’s intelligence elements are included within the definition of the “intelligence community.”

Section 441 also codifies the joint decision of the DNI and Attorney General to designate an office within the Drug Enforcement Administration as an element of the Intelligence Community.

##### *Section 442. Authorization of appropriations for Coast Guard National Tactical Integration Office*

Section 442 provides research and development (R&D) appropriation authorization authority to the Coast Guard National Technical Integration Office (NTIO), which is the Coast Guard counterpart to the Tactical Exploitation of National Capabilities programs in each of the military services. The NTIO explores the use of national intelligence systems in support of Coast Guard operations. Section 442 is intended to enable the National Technical Integration Office to monitor the development, procurement, and management of tactical intelligence systems and equipment and to conduct related research, development, and test and evaluation activities within the context of the Coast Guard’s existing R&D authority.

##### *Section 443. Retention and relocation bonuses for the Federal Bureau of Investigation*

Section 443 makes permanent the authority of the Director of the FBI to pay bonuses to retain certain employees, such as those who have unusually high or unique qualifications or who are likely to leave the Federal service, and to pay relocation bonuses to employees who are transferred to areas in which there is a shortage of critical skills.

##### *Section 444. Extending the authority of the Federal Bureau of Investigation to waive mandatory retirement provisions*

Existing law permits agencies to exempt law enforcement officers from mandatory retirement (generally applicable at age 57 with 20 years of service) until age 60. Under 5 U.S.C. 8335(b)(2), pertaining to the Civil Service Retirement System, and 5 U.S.C. 8425(b)(2), pertaining to the Federal Employee Retirement System, the Director of the FBI may exempt FBI officers from mandatory retirement until age 65, if such an extension is in the public interest. Section 444 extends the waiver authority, which expires at the end of 2009, until the end of 2011.

*Section 445. Report and assessments on transformation of the intelligence capabilities of the Federal Bureau of Investigation*

Section 445 requires the Director of the FBI, in consultation with the DNI, to submit to the congressional intelligence committees, not later than 180 days after enactment of this Act, a report describing the long-term vision for the intelligence capabilities of the FBI's National Security Branch, a strategic plan for the National Security Branch, and the progress in advancing the capabilities of the branch. Among other things, the report is to include a description of the intelligence and national security capabilities that will be fully functional within the 5-year period beginning on the date the report is submitted and a description of the metrics, timetables, and corrective actions. The report will also describe the activities being carried out to ensure the NSB is improving its performance. In addition, Section 445 requires the DNI, in consultation with the Director of the FBI, to conduct for five years an annual assessment of the NSB's progress based on those performance metrics and timetables.

**TITLE V—REORGANIZATION OF THE DIPLOMATIC TELECOMMUNICATIONS SERVICE PROGRAM OFFICE**

*Section 501. Reorganization of the Diplomatic Telecommunications Service Program Office*

Section 501 provides for the reorganization of the Diplomatic Telecommunications Service (DTS) which is comprised of the Diplomatic Telecommunications Service Program Office (DTS-PO) and the DTS Network. The purpose of the DTS-PO is to establish and maintain a DTS Network that is capable of meeting the worldwide communications service needs of United States Government departments and agencies operating from diplomatic and consular facilities including their national security needs for secure, reliable, and robust communications. Section 501 replaces a reorganization plan enacted in the Intelligence Authorization Act for Fiscal Year 2001, and is formally an amendment to that Act which will appear in Title 22 of the U.S. Code.

Section 501 establishes a Governance Board which shall direct and oversee the activities of the DTS-PO. The Director of OMB shall designate from the departments and agencies that use the DTS Network those departments and agencies whose heads will appoint the Governance Board from among their personnel. The OMB Director shall designate the Chair of the Board from among its five voting members and also designate from among the users of the network the department or agency which shall be the DTS-PO Executive Agent.

The Governance Board shall determine the written arrangements, which may be classified, for managing the DTS-PO. The Board shall have the power to approve and monitor the DTS-PO's plans, services, policies, and pricing methodology, and to recommend to the DTS-PO Executive Agent the Board's approval, disapproval, or modification of the DTS-PO's annual budget requests. The Board will also approve or disapprove of the Executive Agent's nomination of a Director of the DTS Program Office.

Section 501 authorizes two-year appropriations for the DTS-PO. It requires that the DTS-PO shall charge only for bandwidth costs

attributable to a department or agency and for specific customer projects.

In requesting enactment of Section 501, the DNI advised the Committee as follows about its purpose: “The appropriations authorized by this measure will promote modernization of the [DTS] network and the expansion of its architecture. With the authority to recover bandwidth costs, the DTS–PO can vastly improve the overall business management and effectiveness of DTS–PO operations. The measure will facilitate the establishment of a financial management system that employs a single system of records, that increases transparency and traceability in customer billing, that promotes responsiveness to customer requirements, that insures timely acquisition of bandwidth and receipt of vendor payments, and that promotes cost-conscious behavior among DTS–PO customers.”

## TITLE VI—FOREIGN INTELLIGENCE AND INFORMATION COMMISSION ACT

### *Section 601. Short Title*

Title VI of the bill establishes a Foreign Intelligence and Information Commission (“the Commission”) to provide recommendations to improve foreign intelligence and information collection, analysis, and reporting through the strategic integration of the Intelligence Community and other elements of the United States Government. Section 601 provides that this title may be cited as the “Foreign Intelligence and Information Commission Act.”

### *Section 602. Definitions*

Section 602 provides definitions, including subsection 602(5) which defines “information” to include information of relevance to the foreign policy of the United States collected and conveyed through diplomatic reporting and other reporting by personnel of the Government of the United States who are not employed by an element of the Intelligence Community, including public and open-source information.

### *Section 603. Findings*

Section 603 provides findings of Congress. Among the findings are: accurate, timely, and comprehensive foreign intelligence and information are critical to the national security of the United States and the furtherance of the foreign policy goals of the United States; and it is in the national security and foreign policy interests of the United States to ensure the global deployment of personnel of the Government of the United States who are responsible for collecting and reporting foreign intelligence and information, including personnel from the Intelligence Community, the Department of State, and other agencies and departments of the Government of the United States, and that adequate resources are committed to effect such collection and reporting.

### *Section 604. Establishment and functions of the Commission*

Section 604 sets forth the functions of the Commission to include evaluating any current processes or systems for the strategic integration of the Intelligence Community, including the Open Source

Center, and other elements of the United States Government, including the Department of State, with regard to the collection, reporting and analysis of foreign intelligence information; providing recommendations to improve or develop such processes or systems to include the development of an inter-agency strategy; and providing recommendations on how to incorporate into the inter-agency strategy the means to anticipate future threats, challenges, and crises, including by identifying and supporting collection, reporting and analytical capabilities which are global in scope and which are directed at emerging, long-term, and strategic threats.

The functions of the Commission also include providing recommendations related to the establishment of any new Executive branch entity, or the expansion of the authorities of any existing Executive branch entity, as needed to improve the strategic integration of foreign intelligence and information collection, reporting and analysis capabilities and oversee the implementation of the inter-agency strategy; and providing recommendations on any legislative changes necessary to establish any new entity or to expand the authorities of any existing entity.

In addition, the functions of the Commission include providing recommendations on strategies for sustaining human and budgetary resources to effect the global collection and reporting missions identified in the inter-agency strategy, including the repositioning of collection and reporting capabilities; and providing recommendations on processes for developing and presenting to Congress budget requests for each relevant element of the United States Government that reflect the allocations identified in the inter-agency strategy and for congressional oversight of the development and implementation of the strategy.

*Section 605. Members and staff of the Commission*

Section 605 establishes that the Commission shall be composed of 10 members, to include two members appointed by the majority leader of the Senate, two members appointed by the minority leader of the Senate, two members appointed by the Speaker of the House of Representatives, two members appointed by the minority leader of the House of Representatives, one nonvoting member appointed by the Director of National Intelligence, and one nonvoting member appointed by the Secretary of State.

Members of the Commission shall be private citizens with: knowledge and experience in foreign information and intelligence collection, reporting, and analysis; knowledge and experience in issues related to the national security and foreign policy of the United States gained by serving in the Department of State, other appropriate agency or department or independent organization with expertise in the field of international affairs; or knowledge and experience with foreign policy decision making. The members of the Commission shall designate one of the voting members to serve as chair.

Subsection 605(b) provides for the staff of the Commission and the selection of an Executive Director.

*Section 606. Powers and duties of the Commission*

Section 606 provides the powers and duties of the Commission, including holding hearings, receiving evidence, and issuing and enforcement of subpoenas.

*Section 607. Report of the Commission*

Section 607 provides that no later than one year after the appointment of members, the Commission shall submit an interim report to the congressional intelligence committees. No later than 4 months thereafter, the Commission shall submit a final report to the President, the Director of National Intelligence, the Secretary of State, the congressional intelligence committees, and the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

*Section 608. Termination*

Section 608 provides that the Commission shall terminate 60 days after the submission of the Commission's final report.

*Section 609. Nonapplicability of Federal Advisory Committee Act*

Section 609 provides that the Federal Advisory Committee Act (5 U.S.C. App.) does not apply to the Commission.

*Section 610. Funding*

Section 610 authorizes that of the amounts available for the National Intelligence Program for fiscal year 2009, \$4,000,000 shall be available for transfer to the Commission.

## TITLE VII—TECHNICAL AMENDMENTS

*Section 701. Technical amendments to the Foreign Intelligence Surveillance Act of 1978*

Section 701 makes technical amendments to the Foreign Intelligence Surveillance Act of 1978 to correct typographical and grammatical errors.

*Section 702. Technical amendments to the Central Intelligence Agency Act of 1949*

Section 702 amends Section 5(a)(1) of the CIA Act of 1949 by striking or updating outdated references to the National Security Act of 1947. The Intelligence Reform Act significantly restructured and renumbered multiple sections of the National Security Act of 1947, leaving references in Section 5(a)(1) of the CIA Act to provisions that no longer exist or that are no longer pertinent.

*Section 703. Technical amendments to Title 10, United States Code*

Section 703 amends Section 528(c) to update references to the names of positions at the Central Intelligence Agency.

*Section 704. Technical amendments to the National Security Act of 1947*

Section 704 corrects and updates technical anomalies in the National Security Act of 1947 arising in part from the amendments made to that Act by the Intelligence Reform Act. Among other provisions, Section 704 amends Section 3(4)(L) of the National Security



rity Act of 1947 (50 U.S.C. 401a(4)(L)) to permit the designation as “elements of the intelligence community” of elements of departments and agencies of the United States Government whether or not those departments and agencies are listed in Section 3(4).

*Section 705. Technical amendments relating to the multiyear National Intelligence Program*

Section 705 updates references to the “multiyear national foreign intelligence program” in the National Security Act of 1947 to incorporate and reflect organizational and nomenclature changes made by the Intelligence Reform Act.

*Section 706. Technical amendments to the Intelligence Reform and Terrorism Prevention Act of 2004*

Section 706 makes a number of technical and conforming amendments to the Intelligence Reform Act.

*Section 707. Technical amendments to the Executive Schedule*

Section 707 makes technical amendments to the Executive Schedule to correct outdated and incorrect references. This section substitutes the “Director of the Central Intelligence Agency” for the previous reference in Executive Schedule Level II to the “Director of Central Intelligence.” See 5 U.S.C. 5313. Section 507 also strikes outdated references to Deputy Directors of Central Intelligence from Executive Schedule Level III. See 5 U.S.C. 5314. The provision also corrects the erroneous reference to the “General Counsel to the National Intelligence Director” in Executive Schedule Level IV. See 5 U.S.C. 5315.

*Section 708. Technical amendments to section 105 of the Intelligence Authorization Act for Fiscal Year 2004*

Section 708 changes the reference to the Director of Central Intelligence to the DNI in Section 105 of the Intelligence Authorization Act for Fiscal Year 2004 (Public Law 108–77 (December 13, 2003)) to clarify that the establishment of the Office of Intelligence and Analysis within the Department of the Treasury, and its reorganization within the Office of Terrorism and Financial Intelligence (Section 222 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 Division H, Public Law 108–447 (December 8, 2004)), do not affect the authorities and responsibilities of the DNI with respect to the Office of Intelligence and Analysis as an element of the Intelligence Community.

*Section 709. Technical amendments to section 602 of the Intelligence Authorization Act for Fiscal Year 1995*

Section 709 changes references to the Director of Central Intelligence in Section 602 of the Intelligence Authorization Act for Fiscal Year 1995 to the Director of National Intelligence or to the Director of the Central Intelligence Agency as appropriate.

*Section 710. Technical amendments to section 403 of the Intelligence Authorization Act, Fiscal Year 1992*

Section 710 makes technical amendments to Section 403 of the Intelligence Authorization Act, Fiscal Year 1992, to reflect the cre-

ation of the position of the Director of National Intelligence and the appropriate definition of the Intelligence Community.

COMMITTEE COMMENTS

*Leadership of the Intelligence Community*

The National Security Act of 1947 is clear. As amended by the Intelligence Reform Act, the Director of National Intelligence is the “head of the intelligence community.” 50 U.S.C. §403(b)(1). With respect to the CIA, the DNI’s authority is direct and immediate. Under the heading of “Supervision,” the Act provides that “[t]he Director of the Central Intelligence Agency shall report to the Director of National Intelligence regarding the activities of the Central Intelligence Agency.” *Id.*, § 403–4(a).

The National Security Act of 1947 specifically addresses coordination with foreign governments. Under the President’s direction, the DNI shall “oversee” the coordination of the relationship between Intelligence Community elements and foreign government or international organization intelligence or security services. *Id.*, § 403–1(k). The CIA has, of course, important responsibilities concerning that coordination but, in keeping with the Act, those responsibilities are to be exercised “[u]nder the direction of the Director of National Intelligence.” *Id.*, § 403–4(f).

Effective May 19, 2009, DNI Dennis Blair, completing a process that began under DNI Michael McConnell, issued Intelligence Community Directive 402 (ICD–402) on the designation by the DNI of DNI representatives to U.S. foreign partners and international organizations. In recognition of the historical overseas role of the CIA, ICD–402 provides that in “virtually all cases globally” the CIA Chief of Station shall serve as the DNI representative to U.S. diplomatic missions. Nevertheless, in “rare circumstances” the DNI, in consultation with Chiefs of Mission, the Director of the CIA, and other affected departments or agencies, may designate a DNI representative other than a CIA Chief of Station.

ICD–402 is faithful to the National Security Act. The DNI is not only the head of the Intelligence Community in Washington, D.C. The DNI is the Community’s head wherever it operates in the world.

The directive recognizes the value of turning to the CIA Chief of Station to be the DNI’s representative in foreign countries, but also recognizes that some locations may give rise to circumstances where that responsibility is best met by an official with expertise derived from another Intelligence Community element, which in fact is already current practice and is not disputed by anyone.

In any event, the DNI, exercising his authority under the law, has made the decision that the directive is the right choice for the Intelligence Community. The Committee supports the DNI in that choice and looks forward to the CIA’s prompt adherence to his decision.

*Cyber issues*

Cybersecurity is a serious national security and economic security challenge of great complexity, deserving of increased attention from the Congress. Because the Comprehensive National Cybersecurity Initiative (CNCI) in 2008 assigned the DNI and Intelligence

Community components key national roles in cybersecurity, the Committee has invested significant time assessing the cyber threat to our country and potential government responses through scores of Member meetings and staff briefings with government, private sector, academic, and nonprofit thought-leaders, six full-Committee closed cyber hearings in the last two years, four six-month studies by the Committee's Technical Advisory Group, and regular outreach to other congressional committees. The reporting requirements in Section 340 are, in part, to encourage continued dialogue with the Executive branch on these issues.

Recently, the Committee closely followed and offered comments on the Administration's 60-day Cyberspace Policy Review directed by the President. The Committee appreciates the White House's effort to be transparent and open with Congress and has high expectations for continued healthy cooperation. The Committee looks forward to building on the current portfolio of CNCI projects, with course-corrections where necessary, and to developing longer-term strategies for national cybersecurity.

Though the Committee continues to deliberate in classified sessions, a few cyber-related observations and concerns can be mentioned here. First, the Committee is troubled by the lack of situational awareness about the opportunities, activities, and identities of cyber thieves or potential attackers on U.S. information networks. This is a serious weakness and a source of frustration for those responsible for oversight and strategic decision-making. Unfortunately, it will not be easy to remedy this, as incentives to report cyber intrusions and vulnerabilities are generally negative in the U.S. government and private sector. The Committee believes this must change so that cybersecurity leaders can make well-informed decisions and respond to problems quickly.

Next, it is clear that cybersecurity activities must be conducted with an expectation of particularly strong congressional oversight that will require solid Executive branch planning before funding for multi-billion dollar programs are authorized and appropriated. In addition, there must be a rigorous analysis of the government's use of legal authorities for national cybersecurity missions that preserve the reasonable privacy expectations of U.S. persons. The government's role must be well-defined as activities involving the Internet evolve.

The Committee seeks an effective governance model for the management of cybersecurity expenditures and operations, with a clear relationship among homeland security, intelligence, military, foreign policy, law enforcement, and other components involved in cybersecurity. It must be clear which government leaders are to be held accountable for new cybersecurity activities. Further, the Committee expects the President to provide a clear vision, strategic direction, and effective integration of the wide range of cybersecurity activities.

The federal government's communication strategy concerning cybersecurity must be improved as well. The prior reluctance to invite Congress into the cybersecurity debate in a timely manner was to the detriment of what could have been a more cooperative and productive interaction between the branches. Also, the Committee believes there should be a new plan on the best way to communicate the national cybersecurity policy to the public. Though some

elements must be classified, it is important that the U.S. people understand the government's basic role in helping to secure information networks. The general rules and expectations for government involvement, and how these may affect privacy, must be clearly explained.

In addition, the government must consider international relations and how our country's intentions are transmitted overseas. Indeed, the Committee supports stronger international outreach with traditional allies and other key nations to develop consensus on what cyber activities will be promoted, tolerated, and censured. An international framework on cyber warfare, much like international conventions on traditional warfare, is needed to govern this rapidly growing field.

The Committee believes there should be a significant emphasis in the government's cyber investment portfolio on long-term issues such as research and development (R&D), recruiting experts into government, and education and training. In particular, recent studies sponsored by the Committee have concluded that the Intelligence Community must dramatically increase funding for R&D in order to be effective in the future. The cyber technology world is moving quickly, with cutting-edge technology expertise spread across the globe, and the United States cannot presume a clear-cut technology advantage as it has in other areas of national security. The Committee recommends a balanced portfolio approach that includes a nationally coordinated program of long-term, high-risk research aimed at revolutionary breakthroughs, sustained even when faced with near-term budget pressures. The Committee strongly supports a rebalancing of the CNCI budget to address these concerns.

Finally, as a step beyond the CNCI's focus on securing federal government information networks, the Committee is highly concerned about protecting the U.S. critical infrastructure. For example, the country's electric power grid, communications systems, and financial infrastructure are all critical to our way of life yet unacceptably vulnerable to cyber attack. The government and the private sector must work together to share more effectively cyber threat and vulnerability information, and the Administration and the Congress must work together to determine the best mix of mandates, incentives, and other tools to improve critical infrastructure security. The Committee also supports recent recommendations from its Technical Advisory Group stressing the importance of a survivable government communications network to sustain critical national security functions under and following major cyber attack.

In addition, the Committee requests the following near-term actions for the Administration. As requested in a March 23, 2009, letter from the Chairman and Vice Chairman of the Committee to the DNI, the Committee recommends that the Administration propose legislation giving the Director of National Intelligence primary authority to manage all aspects of cybersecurity pertaining to any Intelligence Community communication and information system. This should include the ability to mandate red-team penetration testing, using any Intelligence Community red team, on any Intelligence Community communication or information system at any time, with test results reportable to the Director of National Intelligence.

Also, the Committee recommends that the DNI, in consultation with the OMB, implement a system (“dashboard”) to provide dynamic, comprehensive, real-time cybersecurity status and vulnerability information of all Intelligence Community communication and information systems to the DNI.

To ensure that cybersecurity best practices spread through the entire Intelligence Community enterprise, the Committee requests that the DNI: (1) direct an Intelligence Community cybersecurity awareness campaign that covers all Intelligence Community employees and contractors; (2) direct that cybersecurity become a significant part of the performance and bonus evaluations for all Senior Intelligence Service (SIS) members; and (3) create a Secure Products and Services Acquisitions Board, responsible for ensuring all Intelligence Community purchases meet standards for cybersecurity as established by the Board. For this last recommendation, the Committee notes that its intent is not to create another time-consuming approval layer and slow acquisitions; the Board should adjudicate in a timely manner, or not at all.

Beyond Intelligence Community issues, the Committee is interested in accelerating the growth of the national cyber investigative and law enforcement capabilities, toward the goal of improved national ability to attribute and prosecute cyber adversaries. Therefore the Committee recommends that the DNI increase support for the National Cyber Investigative Joint Task Force and ensure appropriately cleared, full-time staff are detailed to the Task Force with complete access to any intelligence information that could support cyber investigations on foreign adversaries.

Also, the Committee recommends that the DNI and the Secretary of Homeland Security perform a joint, comprehensive, up-to-date assessment of risk due to cyber threats to and cyber vulnerabilities in the U.S. critical infrastructure and submit a report on this assessment to Congress by January 1, 2010. The assessment should consider all types of cyber threats, of domestic or foreign origin, particularly those to U.S. electric power command and control systems, and all types of cyber vulnerabilities, and combine them to create the risk assessment.

Finally, the Committee supports recent recommendations from its Technical Advisory Group that the Administration should consider changes to U.S. immigration policy that would offer expedited citizenship to certain foreign nationals studying in the United States who graduate with degrees in science, technology, engineering, and mathematics, with particular focus on computer science.

#### *Foreign language capability of the Intelligence Community*

The Committee is concerned about the abysmal state of the Intelligence Community’s foreign language programs. The collection of intelligence depends heavily on language, whether information is gathered in the field from a human source or from a technical collection system. Even traditionally nonlinguistic operations such as imagery rely on foreign language skills to focus and direct collection efforts. But almost eight years after the terrorist attacks of September 11th and the shift in focus to a part of the world with different languages than previous targets, the cadre of intelligence professionals capable of speaking, reading, or understanding crit-

ical regional languages such as Pashto, Dari or Urdu remains essentially nonexistent.

Section 1041 of the Intelligence Reform Act required the DNI to identify the linguistic requirements of the Intelligence Community, and to develop a comprehensive plan to meet those requirements. Five years later, the ODNI has still not completed an IC-wide comprehensive foreign language plan that designates specific linguist or language requirements, lays out goals or timelines, or designates specific actions required to meet them.

Furthermore, individual agency and military service programs aimed at creating strategies to improve foreign language programs are inconsistent across the Intelligence Community. NSA has near-real-time visibility of its language-capable employees and hires and trains according to actual needs, but most other Intelligence Community agencies have no similar capability. The new Director of the CIA recently announced a major overhaul of the CIA's foreign language hiring, training, maintenance, and use policies which should eventually result in a more language capable workforce, but other agencies have not been similarly aggressive. DIA continues to suffer from chronic shortages of language-capable employees, but has not developed a strategy for improvement. To explain their failure to redress critical gaps in national security foreign language capacity, agencies point to their lack of control over clearance processes, shallow hiring pools, the inability to allocate time to training, insufficient resources, and, in some cases, a dearth of qualified instructors. Yet, the United States is one of the most polyglot of developed countries—more than one in five Americans speak a language other than English in the home and more than a million citizens are of Middle East or South Asian descent.

The Committee is concerned that persistent critical shortages in some languages contribute to the loss of intelligence information and affect the ability of the Intelligence Community to process and exploit what it does collect. This seriously hampers the nation's ability to engage constructively and appropriately overseas.

The Committee expects to receive by the end of this year a comprehensive strategy for improving foreign language capabilities across the Intelligence Community, including but not limited to meeting the requirements for translators, interpreters, collectors, analysts, liaison officers and attaches. The Committee has provided additional resources to address this perpetual shortcoming in Section 306 and as discussed in the classified annex.

#### *Intelligence Community core contract personnel*

The Committee remains concerned over the number of contract personnel engaged in core activities in the Intelligence Community. For the last three years, the IC CHCO has gathered data and presented analysis on the number and cost of these core contract personnel. The most recent Intelligence Community Core Contract Personnel Review for 2008 found that core contract personnel made up 29 percent of the total Intelligence Community personnel yet represented 49 percent of the total personnel budget. Overall, the Intelligence Community reduced its use of contract personnel for these core positions by 3 percent last year. The NRO and NGA, however, had considerable growth in their contract personnel ranks in 2008.

While recognizing that core contract personnel may be necessary for short-term assignments or to allow intelligence agencies to acquire unique expertise, the Intelligence Community agencies themselves have determined that many of the functions currently performed by contract personnel can be successfully performed by government employees at a considerable savings to the government. The CIA in particular has taken a leadership role in identifying these positions, converting contract personnel into agency employees, and redirecting the resulting savings to more productive uses.

As set forth in Section 103 of the bill, the Committee recommends that the Intelligence Community agencies be authorized to convert their contract personnel positions into civilian employees. The Committee believes the IC CHCO has been conducting important oversight in bringing uniform personnel procedures to the Intelligence Community and requiring the intelligence agencies to analyze their usage of contract personnel. These are important steps that must be taken before determining the correct size and composition of the Intelligence Community workforce today and in the future.

Nevertheless, the Committee believes the Intelligence Community should further reduce its dependence on contract personnel. Therefore, the Committee directs that the Intelligence Community reduce its core contract personnel by at least 5 percent below the level requested for fiscal year 2010.

*Information Integration and the Intelligence Community Chief Information Officer*

The Committee was impressed with the vision and accomplishments of the Information Integration Program (I2P). The I2P was initiated in the summer of 2008 as an informal means of determining areas within the Intelligence Community's information technology systems that could be altered to better enable information sharing and access, and then providing the guidance and resources to enable these changes to take place. Unlike similar efforts in the private sector which are driven by cost savings, I2P had a primary goal of demonstrating how improved connectivity between and among intelligence agencies could help Intelligence Community components perform their mission better. While cost savings may be an ancillary benefit, the mission focus of I2P proved to be an attractive motivation for Intelligence Community personnel.

Almost eight years after the attacks of September 11th, and five years after its creation by passage of the Intelligence Reform Act, the ODNI has found a process to build links among communication systems and to develop common information technologies and standards—the infrastructure on which intelligence information can be shared and accessed. As improved information sharing had been a fundamental rationale for creating the DNI, these improvements are long overdue. Intelligence Community Directive 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, issued by the DNI on January 21, 2009, sets forth new policies that establish the “responsibility to provide” information to authorized personnel and a framework to implement this policy. Taken together, the Committee believes these actions will create a fundamental change in how intelligence collection and

analysis may be distributed, if appropriate, among and between intelligence agencies, the U.S. government, state and local authorities, and the general public.

Despite the substantial promise of I2P's reforms, the Committee had been concerned that the effort might disappear once the individuals leading I2P moved on, given its ad hoc nature within the ODNI. Therefore, the Committee supports the decision by the DNI to continue the I2P reforms through the IC CIO and believes the IC CIO's primary mission should be to continue and build upon the I2P effort. Additionally, the Committee has recommended a fence on enterprise management information technology funds requested for each agency pending certification by the IC CIO that an agency is addressing specific issues related to the I2P effort. Further, the Committee expects the IC CIO to continue to provide quarterly update briefings on the initiatives begun under I2P to the congressional intelligence committees as this effort progresses.

*Need for increased and stable research and development funding*

The Committee remains concerned about the chronic underfunding of research and development in the Intelligence Community. The Intelligence Community has traditionally developed its own advanced technologies rather than looking outside to meet intelligence operational needs. The funds invested in the past for research and development of new technology have made the Intelligence Community the world leader in most technical collection disciplines. Without these investments, the U.S. would be facing much greater risks and threats to its national security. The Committee believes the Intelligence Community must retain its technological edge.

Last year, the Administration's National Intelligence Program budget request devoted only 3 percent of the total request to R&D. Congress added significant funding for R&D to the National Intelligence Program request in the fiscal year 2009 appropriations. The Administration, however, did not sustain these increases and the fiscal year 2010 National Intelligence Program request again only has 3 percent of the total request directed towards research and development.

The Committee does not support the established budgetary practice of raiding R&D accounts to address short-term budget problems within the Intelligence Community. While not unique to the Intelligence Community, the chronic underfunding of R&D programs will have long-term effects on the ability of the United States to know what adversaries are planning and to protect its citizens from these threats. In particular, the Committee is seriously concerned with the NRO's decision to reduce its R&D funding from 8 percent of the budget in fiscal year 2006 to just 6 percent of its budget in fiscal year 2010. For an organization whose mission is focused on advanced technical collection of intelligence, these cuts are puzzling and short-sighted.

Despite the inadequate funding request for R&D, the Intelligence Community has made some progress in promoting advanced research and development through the establishment of the Intelligence Advanced Research Projects Agency (IARPA). Similar to the Department of Defense Advanced Research Projects Agency (DARPA), which developed the Internet and Predator UAVs, the



IARPA has the charge to identify, nurture, and promote long-term R&D projects with the potential to alter fundamentally intelligence collection and analysis. The Administration, however, did not sustain the substantial increases Congress approved for IARPA in fiscal year 2009 in this year's budget request.

The Committee recommends increases in the National Intelligence Program budget for R&D spending to 4 percent of the total Intelligence Community budget and believes the Intelligence Community should sustain and eventually increase this funding to 5 percent of the total National Intelligence Program budget in next year's budget request.

#### *Intelligence Community financial management*

The Intelligence Community must be able to produce financial reports that pass independent audit if the taxpayers and Congress are to have confidence that the National Intelligence Program budget, which was \$47.5 billion for fiscal year 2008, is being spent effectively. The Committee formally began advocating for increased Intelligence Community compliance with federal financial accounting standards in September 2001. The report language accompanying the Committee's Fiscal Year 2002 Intelligence Authorization bill noted that as early as January 1997, the President had called for selected Intelligence Community agencies to begin producing classified financial statements. The report language called for the financial statements of the NRO, NSA, CIA, DIA, and what is now the NGA to be audited by a statutory Inspector General or independent public accounting firm by March 1, 2005. The intent was that by that time, the statements would be auditable.

Progress over the last decade toward the goal of auditable financial statements has been woefully insufficient. Since September 2001 each agency has overstated its progress in establishing the processes, procedures, and internal controls that would allow for the production of auditable statements. These promises have been accompanied by the hiring of multiple contract personnel who have created numerous studies and plans that have often been duplicative and merely pointed out the obvious. There has also been a lack of senior management attention to the need for improved financial accountability. One symptom of this inattention is the existence of over a dozen long-standing, correctable, material weaknesses, which pose serious obstacles to financial auditability. To ensure clear accountability and to focus senior management attention on their correction, Section 359 requires the heads of the CIA, DIA, NGA, NRO, and NSA to designate each senior management official who is responsible for correcting these weaknesses, and to notify the DNI and the congressional intelligence committees of these designations.

The NRO received a favorable audit opinion auditable financial statement in fiscal year 2003, but since then has slipped to the point of not doing an audit of its fiscal year 2007 statement pending further improvements to internal processes. The NSA put into operation a new commercial off-the-shelf financial management system, which also supports the DIA, but, as the Chairman and Vice Chairman pointed out in a March 9, 2009, letter to the DNI, the NSA grossly mismanaged the implementation of the system. The NGA was scheduled to move to this NSA-DIA accounting sys-

tem, but that move is on hold pending resolution of NSA's implementation problems and IC-wide business system architecture deliberations coordinated by the DNI's new Business Transformation Office (BTO). The bottom line is that more than ten years after the President called for action, and more than four years after the Committee anticipated receiving auditable statements, the five agencies are still unable either to produce auditable financial statements or receive favorable audit opinions on those that are auditable. The current projection for doing so is at least four years away.

The first, and so far only, serious IC-wide plan for producing auditable statements is contained in an April 2007 DNI report titled *Financial Statement Auditability Plan*. The report outlined the current state of the Intelligence Community's financial management systems, explained the challenges to achieving unqualified audit opinions, and specified key milestones for each agency on the path to clean audit opinions in fiscal year 2012. The report failed, however, to explain how independent audit assessments of important milestones would be conducted, and it contained no plan for when individual agency systems could be merged into an IC-wide business enterprise architecture (BEA).

Accordingly, the April 2007 plan has now been superseded by the imperative to construct a BEA, which makes the 2012 auditability timeline difficult or impossible to achieve for most agencies. Nonetheless, the Committee strongly supports this BEA work, which, if successful, will provide a stronger foundation for sustainable, financial auditability. Indeed, the Committee has repeatedly called for a BEA over the last four years. Section 322 of this bill is designed to empower the DNI's fledgling BTO to produce this business systems architecture. The Committee strongly believes that a separate BTO, staffed with officers with relevant experience, is indispensable to progress towards the BEA—as a similar office has shown to be in the Department of Defense. Accordingly, the Committee would view as unwise and counterproductive any dilution of the BTO. The Committee awaits the next major milestone in the BTO's efforts to construct an effective BEA, the December 31, 2009, delivery of the rigorous BEA framework mandated by the Committee.

Nonetheless, the BTO's work must not delay sorely-needed improvements to internal controls, which are critical to preventing millions of dollars of potential fraud, waste, and abuse, as well as providing reliable business information for sound decision-making. Many of these process controls do not need to await the result of BTO's architectural deliberations. We therefore urge the DNI and Intelligence Community agency heads to take strong and decisive action to see that appropriate reforms and oversight controls are in place as soon as possible.

Finally, the Committee believes that both the Congress and the DNI would benefit from the creation of a consolidated National Intelligence Program financial statement. Such a statement would provide valuable macro-level data and, once established, offer insight into financial trends within the Intelligence Community. Therefore, the Committee requests that the DNI begin preparing a consolidated financial statement for the National Intelligence Program beginning with fiscal year 2011. In accordance with the DNI's

*Financial Statement Auditability Plan*, this statement should be based on the fully auditable data provided by each of the Intelligence Community agencies. As such, a separate audit will not be required for the consolidated statement.

*Resource Management and the Chief Financial Officer for the Intelligence Community*

It is widely recognized that the Intelligence Community's process for generating requirements for major acquisitions is broken. For instance, as the Committee has noted previously, a significant percentage of major acquisition programs have not been linked to providing intelligence requirements that have been formally validated. Moreover, the process of identifying intelligence requirements is not sufficiently linked to budgetary constraints, leading to budget requests that include more programs than can sustainably be funded. To remedy this situation, budgetary constraints need to be explicitly considered throughout the entire resource process. In addition, the Chief Financial Officer in the ODNI, whose responsibility it is to prepare a budget for the DNI, needs to be centrally involved throughout the *entire* decision-making process—not just the budgeting at the end of the process.

By the ODNI's own assessment, the current resource management process is "fragmented, unsynchronized, complex, and opaque." Past efforts to address this problem have been ineffective and set aside.

The Committee applauds the current DNI's efforts to perform more rigorous, quantitative, long-term analyses of resource issues. To lead this effort, he has established a new Associate Director of National Intelligence for Systems and Resource Analyses. The Committee is concerned, however, that creating yet another senior resource position further balkanizes an already fragmented resource process.

Unless one senior officer has *exclusive* responsibility for end-to-end resource management, resource decisions will continue to be slow, needlessly complex, subject to contentious revisits, and certainly not integrated. One, and only one, senior officer reporting to the DNI must be in charge and accountable. Therefore, Section 408 of the bill creates the position of the IC CFO, investing that position with the duties, responsibilities, and authorities of the CFO Act of 1990, as appropriate. The section makes clear that the IC CFO will serve as the principal advisor to the DNI on Intelligence Community budgetary resources, and that this officer will establish and oversee a comprehensive and integrated strategic process for managing Intelligence Community resources. Other senior officers may be primarily responsible for certain aspects of this overall process, such as strategic planning, long-range investment analysis, independent cost estimation, or acquisition milestone decision authority, but Section 407 makes the IC CFO responsible for the coordination of all resource processes. The Committee intends and expects that, as the principal advisor to the DNI on resource allocation, the IC CFO will consider and balance the equities of all Intelligence Community parties in his or her recommendations to the DNI, and that the DNI in turn, will receive recommendations directly from the IC CFO.

*Independent cost estimation*

The Committee believes that the greater number of intelligence programs that are subjected to the discipline of an Independent Cost Estimate (ICE) or other independent cost assessment, the more financially realistic and sustainable the National Intelligence Program budget becomes. Therefore, the bill reduces the threshold cost of a program from \$500 million to about \$170 million before an ICE is required. This threshold is used throughout the U.S. government to define a major system acquisition, and its adoption in the bill responds to the ODNI's request to make this definition uniform in statute. The Committee anticipates that the ODNI's Intelligence Community Cost Analysis and Improvement Group (IC CAIG) will delegate many of the resulting additional ICEs for smaller programs to those executing agencies with independent cost estimating capabilities. The Committee also strongly encourages the IC CAIG to continue to expand its purview to large programs that are not usually considered "systems acquisition," such as Intelligence Community data centers, the pending cyber initiative, and large personnel increases that function together to fulfill a mission need.

Also, while the Committee is impressed with the professionalism and productivity of the IC CAIG, it believes it is incumbent on the IC CAIG to establish and publish the track record of its ICEs in predicting actual program costs. Accordingly, the Committee requests that future budget requests or annual Program Management Plan Reports include a comparison of all IC CAIG ICEs to the actual costs of completed and ongoing programs. The comparison should be on a basis that is consistent from year to year and from program to program. Such a comparison may account for changes in program scope, but it should also compare estimates to actual costs without scope changes. The Committee recommends that the IC CFO consult with the Committee on its proposed methodology for establishing such a track record prior to its publication in the congressional budget justification books.

*Performance based budgeting: major progress made in FY 2010 Budget*

This year's FY 2010 National Intelligence Program budget request builds on last year's progress in performance-based budgeting. It represents the first full performance budget, providing the Committee valuable new information for oversight. The Committee is especially pleased that the improvements it urged last year in the performance budget for counterterrorism have been made. The Committee also applauds the ODNI's adoption of facility condition index metrics, CIA's advancement of measures for HUMINT and covert action performance, and the NRO's use of functional availability as a performance methodology. Even so, the DNI and the Intelligence Community are years behind much of the rest of the government. The quality of the measures, targets, performance assessments, and linkage to funding is highly uneven. In addition, too often the performance information appears to be an administrative after-thought to the budget rather than an integral part of its development. As the government-wide fiscal picture tightens, it will be increasingly incumbent on the Intelligence Community to justify its resource requests on the basis of improved performance.

*Principal Deputy Director of National Intelligence*

The Principal Deputy Director of National Intelligence position was established as a Presidentially-appointed, Senate-confirmed position by the Intelligence Reform Act, but has been filled by a confirmed individual for barely half of the intervening four years. The Office was vacant for over a year from 2006 to 2007, and has been vacant again since January 2009. As of the date of filing this report, no nomination for this position is pending.

The Principal Deputy position is among the most important in the Intelligence Community. The Principal Deputy is charged with assisting the DNI in the performance of the DNI's duties, and of exercising the DNI's authorities and carrying out the DNI's responsibilities when the DNI is absent or when the DNI position is vacant. While the Committee does not wish to fault the performance of either the incumbent DNI or the incumbent Acting Principal Deputy, it notes that the Principal Deputy position was created because Congress believed that leading the Intelligence Community was a job which required that the DNI be assisted by a confirmed, full-time appointee, rather than an acting appointee who has other full-time job responsibilities. Moreover, the intention of the Congress, and the law that it enacted, is that a confirmed Principal Deputy would stand ready to act as the DNI in the event that a vacancy occurred so there would be no gap in the leadership of the Intelligence Community.

The Intelligence Reform Act states that when the Principal Deputy position is vacant the DNI shall recommend an individual for appointment. The Committee hopes to receive a nomination for this position from the President in the very near future.

*National Counterterrorism Center*

The Committee receives regular briefings on terrorism threats from intelligence analysts at the NCTC and commends the Center for its continued success in improving the quality of their briefings and intelligence products. The Committee looks forward to additional advances in quality as the NCTC matures. The Committee is also encouraged by recent improvements in the NCTC's Department of Strategic Operational Planning, a function the Committee will continue to focus on throughout 2009 and 2010.

The Committee understands that NCTC has developed an effective mechanism for sharing intelligence information among personnel serving at the Center, but that there continues to be concern among counterterrorism analysts serving at the individual intelligence agencies about the degree to which they have access to relevant terrorism-related intelligence information from other agencies. The Committee will continue to look into this issue as the bill is considered by the Congress.

*Defense Intelligence Agency—Counterterrorism Analysis*

The DIA details a significant number of its counterterrorism analysts on rotations to support the missions of other commands, agencies, organizations, deployed forces, and the NCTC. The Committee is concerned that many of these analysts—particularly those assigned to NCTC—do not return to the Joint Intelligence Task Force-Combating Terrorism or another DIA office upon completion of this rotational assignment, and instead chose to leave DIA.

Therefore, the Committee requests that the Director of the DIA undertake a study to examine factors that may lead analysts who undertake rotational assignments at other agencies or organizations to leave DIA employment, as well as to propose mitigation strategies. The study should be briefed to the Committee no later than December 31, 2009.

*Federal Bureau of Investigation intelligence transformation*

The Committee has closely examined efforts by the FBI to transform its National Security Branch into a premier intelligence and national security organization. While the FBI has made progress in its efforts to fulfill its national security and intelligence mission, the Committee believes the FBI must accelerate its intelligence reform efforts and improve its performance.

In addition, the Committee expects the FBI to increase its transparency and cooperation with Committee oversight. In several instances the FBI has not kept the Committee “fully and currently” informed of its intelligence activities, nor has it responded to Congressional Questions for the Record in a reasonable time frame. While responsibility for this deficiency lies at least partially with the Department of Justice, the Committee adamantly believes the FBI itself must take corrective steps. The Committee requests that a report be provided to the intelligence committees detailing how the National Security Branch of the FBI will improve its cooperation with oversight and align its briefing policies on intelligence matters with the requirements of the National Security Act. The report should be submitted by November 1, 2009. The Committee has fenced a portion of funds, as discussed in the classified annex, until this matter is adequately addressed.

Furthermore, as set forth in Section 445 of the bill, the Committee recommends that the Director of the FBI, in consultation with the DNI, be required to submit a report describing the long-term vision for the intelligence capabilities of the National Security Branch, a strategic plan for the National Security Branch, and details on the progress made to date in advancing the intelligence capabilities of the branch. Section 445 also directs that the DNI, in consultation with the Director of the FBI, submit an annual assessment that tracks the progress of the National Security Branch in strengthening its intelligence capabilities. This report is to be provided to the congressional intelligence committees annually for a period of five years.

*FBI National Security workforce management and the advancement of an FBI analytic culture*

Intelligence Analysts and Professional Staff: The Committee remains concerned that the FBI continues to lack a robust Intelligence Analyst career path. Furthermore, the Committee believes there are too few intelligence analysts in senior positions of responsibility and that the FBI has neglected opportunities to utilize intelligence analysts and other professional staff to fill inherently non-law enforcement, intelligence-focused positions. The FBI was granted authority in the Consolidated Appropriations Act of 2005 to utilize critical pay authority to obtain twenty-four Senior Intelligence Officer (SIO) positions, which were portrayed as “critical to the FBI’s intelligence mission.” In testimony provided to this Com-

mittee on January 25, 2007, the FBI described these SIOs as “senior analysts who will sustain the focus on issues about which policy makers and planners need information now.” As of June 2009, the FBI has hired only six of the twenty-four SIOs. The Committee believes this is unacceptable and that the FBI must do more to advance its non-agent intelligence cadre.

**Special Agents:** The Committee is concerned about the FBI’s continued reliance on Special Agents in the National Security Branch to fill all types of positions and urges the FBI to be more strategic in its deployment and use of special agents. Substantial resources are devoted to providing Special Agents with unique skill sets and their appointments should be made in a manner that is effective and efficient. The Committee believes the use of Special Agents in organizational support functions unrelated to intelligence or law enforcement should be given careful consideration based upon the nature of the particular support function. This is not only cost-effective, but allows for better continuity and strategic positioning of the FBI national security workforce.

#### *Regionalization of the FBI Intelligence Program*

While the FBI has made strides in reforming Field Intelligence Groups, additional reforms are required. Specifically, the Committee believes the FBI should give fuller consideration to the creation of regional intelligence groups, placed organizationally above Field Intelligence Groups, to create an intelligence and national security reporting chain that would be more manageable and accountable.

#### *The state of counterintelligence in the Intelligence Community*

The Committee is concerned about the management, leadership, and focus of the counterintelligence discipline within the Intelligence Community. A number of espionage cases since 2001 have underscored the threat posed by foreign intelligence services to the United States of America. Recent press coverage has highlighted the enduring threat posed by the Cuban intelligence services. The threat from Russia, China, and other nations is no less serious.

An improved approach to counterintelligence will not deter any and all forms of espionage from occurring. However, a heightened counterintelligence posture in the Intelligence Community will better detect and disrupt the sustained threat posed to the US and its interests by foreign intelligence services.

To effectuate meaningful change in counterintelligence, leadership from the DNI is required. Unfortunately, the NCIX is hampered in its ability to execute this leadership role by the authorities assigned to the office and the limited, if any, visibility into counterintelligence operations.

The Committee is supportive of the preliminary steps the DNI has taken by convening a senior panel to review the state of counterintelligence. The DNI should use this opportunity to augment the vital fundamentals of a strong, cohesive counterintelligence posture for the Intelligence Community. This includes enhancing existing counterintelligence training, producing more timely counterintelligence analysis, improving cooperation on counterintelligence operations and analysis between agencies, and more effectively linking counterintelligence and cyber threats.

The Committee looks forward to working with the DNI to improve the state of counterintelligence in the Intelligence Community.

*Department of Homeland Security—Personnel*

Although the Committee commends the Office of Intelligence and Analysis (OIA) of the Department of Homeland Security for recognizing the importance of converting contractor positions to government civilian personnel in fiscal year 2010, the Department's plans to continue a gradual conversion of contract personnel positions to government civilian personnel through 2015, when the workforce mix will be about 50/50, is unacceptable. The Committee has consistently underscored its concerns regarding the long-term use of private contract personnel and the associated costs compared to government civilian employees. Currently, contract personnel make up 63 percent of the workforce of the OIA. The OIA must improve its ratio of contract personnel to government civilian personnel to levels at least comparable to the rest of the Intelligence Community. According to the annual inventory of core contract personnel for fiscal year 2008, issued by the ODNI, contract personnel constitute 29 percent of the Intelligence Community's total personnel. As stated previously, the Committee believes that this figure is substantially above what it should be.

Moreover, the Department of Homeland Security OIA workforce request reflects a disproportionately high percentage increase in total personnel over the past few years. The Committee requests the ODNI work with the next Under Secretary for Intelligence and Analysis to complete a comprehensive study to determine the appropriate number of personnel, define inherently government functions, identify where contract personnel might be performing those functions, and specify how the Office intends to transition contract personnel from those functions within the fiscal year given the statutory mission of the OIA, as described on its website, to "ensure that information related to homeland security threats is collected, analyzed, and disseminated to the full spectrum of homeland security customers in the Department, at state, local, and tribal levels, in the private sector, and in the Intelligence Community."

*Department of Homeland Security—Analysis*

The Committee has raised a number of concerns with reports issued by the Department of Homeland Security OIA that inappropriately analyze the legitimate activities of U.S. persons. These reports raised fundamental questions about the mission of the OIA and often used certain questionable open source information as a basis of their conclusions. The Committee recommends that the next Under Secretary for Intelligence and Analysis conduct a comprehensive review of the quality and relevance of the intelligence products produced by the OIA, and provide this review to the congressional intelligence committees within 180 days of enactment.

*National Immigration Information Sharing Office of the Department of Homeland Security*

The Committee has closely followed the development of the National Immigration Information Sharing Office (NIISO) within the Department of Homeland Security. NIISO is intended to facilitate



the use of citizenship and immigration information currently being collected and housed at a U.S. Citizenship and Immigration Service's facility. Because the NIISO relates to the use of citizenship and immigration information for intelligence purposes, the Congress has been attentive to civil liberties and privacy concerns associated with the NIISO.

According to the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, "[n]one of the funds provided in this or any other Act shall be available to commence operations until the Secretary certifies that such program complies with all existing laws, including all applicable privacy and civil liberties standards, the Comptroller General of the United States notifies the Committees on Appropriations of the Senate and the House of Representatives and the Secretary that the Comptroller has reviewed such certification, and the Secretary notifies the Committees on Appropriations of the Senate and the House of Representatives of all funds to be expended on the National Immigration Information Sharing Operation pursuant to section 503." The Committee endorses this provision and awaits the Secretary's certification.

*Compliance with Senate Rule XLIV*

The bill and classified annex create no earmarks as defined by rule XLIV of the Standing Rules of the Senate, which requires publication of a list of congressionally directed spending items. The bill and classified annex contain no limited tax benefits or limited tariff benefits.

COMMITTEE ACTION

*Vote to report the committee bill*

On July 16, 2009, a quorum for reporting being present, the Committee voted to report the bill, by a vote of 15 ayes and no noes. The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Chambliss—aye; Senator Burr—aye; Senator Coburn—aye; Senator Risch—aye.

*Votes on amendments to committee bill and the classified annex*

On July 15, 2009, by a voice vote, the Committee agreed to a managers' amendment by Chairman Feinstein and Vice Chairman Bond to authorize: (1) additional fulltime equivalent personnel in order to improve proficiency in critical foreign languages (Section 306) (sponsored by Senator Wyden and Senator Chambliss); (2) the DNI to make available CIA acquisition authorities to other elements of the Intelligence Community (Section 326); (3) a requirement for a study and strategy on intelligence collection capabilities against the threat of biological weapons (Section 339) (sponsored by Senator Burr and Senator Mikulski); (4) expenditure authority for the Director of the DIA (Section 434); and (5) a governance structure for the Diplomatic Telecommunications Service Network (Title V). In addition, the amendment narrowed Section 352, relating to

sharing terrorist identification information, and incorporated technical and conforming amendments.

On July 15, 2009, by a voice vote, the Committee agreed to an amendment by Chairman Feinstein as modified concerning classified activities that are further described in the classified annex.

On July 15, 2009, by a vote of 11 ayes to 4 noes, the Committee adopted an amendment by Chairman Feinstein concerning congressional notifications further described in the classified annex. The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Hatch—no; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—aye; Senator Coburn—no; Senator Risch—aye.

On July 15, 2009, by a voice vote, the Committee agreed to an amendment by Chairman Feinstein, Senator Rockefeller, Senator Bayh, Senator Mikulski, Senator Feingold, Senator Whitehouse and Senator Snowe to improve congressional and Executive branch oversight of cyber security activities (Section 340).

On July 15, 2009, by a vote of 9 ayes to 6 noes, the Committee adopted an amendment by Chairman Feinstein pertaining to congressional oversight (Section 331). The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Hatch—no; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—no; Senator Coburn—no; Senator Risch—no.

On July 15, 2009, by a voice vote, the Committee agreed to an amendment by Vice Chairman Bond as modified to require the identification of senior intelligence management officials responsible for correcting long-standing correctable material weaknesses (Section 359).

On July 15, 2009, by a voice vote, the Committee agreed to an amendment by Vice Chairman Bond concerning classified activities that are further described in the classified annex.

On July 15, 2009, by a voice vote, the Committee agreed to a second amendment by Vice Chairman Bond concerning classified activities that are further described in the classified annex.

On July 15, 2009, by a voice vote, the Committee agreed to a third amendment by Vice Chairman Bond concerning classified activities that are further described in the classified annex.

On July 15, 2009, by a vote of 13 ayes to 2 noes, the Committee adopted an amendment by Vice Chairman Bond expressing a Sense of the Senate that a subcommittee on intelligence should be created by the Senate Appropriations Committee (Section 341). The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—no; Senator Nelson—no; Senator Whitehouse—aye; Vice Chairman Bond—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Chambliss—aye; Senator Burr—aye; Senator Coburn—aye; Senator Risch—aye.

On July 15, 2009, by a vote of 8 ayes to 7 noes, the Committee adopted an amendment by Senator Rockefeller concerning congressional notifications (Sections 332 and 334). The votes in person or

by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Hatch—no; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—no; Senator Coburn—no; Senator Risch—no.

On July 15, 2009, by a voice vote, the Committee agreed to an amendment by Senator Wyden and Senator Feingold as modified concerning the Public Interest Declassification Board (Section 357).

On July 15, 2009, by a vote of 8 ayes to 7 noes, the Committee adopted an amendment by Senator Wyden and Senator Feingold concerning Government Accountability Office audits of the Intelligence Community (Section 335). The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Hatch—no; Senator Snowe—no; Senator Chambliss—no; Senator Burr—no; Senator Coburn—no; Senator Risch—no.

On July 15, 2009, by a voice vote, the Committee agreed to an amendment by Senator Chambliss and Senator Bayh as modified concerning classified activities that are further described in the classified annex.

On July 16, 2009, by a vote of 10 ayes to 5 noes, the Committee adopted an amendment by Vice Chairman Bond concerning the publication of unclassified versions of intelligence products (Section 427). The votes in person or by proxy were as follows: Chairman Feinstein—no; Senator Rockefeller—no; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—no; Vice Chairman Bond—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Chambliss—aye; Senator Burr—aye; Senator Coburn—aye; Senator Risch aye.

On July 16, 2009, by a vote of 9 ayes to 6 noes, the Committee adopted an amendment by Senator Feingold and Vice Chairman Bond, that requires the President to disclose to the public the funding level requested for the National Intelligence Program on the date the budget request is submitted and eliminates the provision in current law whereby the President may waive or postpone the disclosure of the aggregate amount of funds appropriated by Congress for the National Intelligence Program on national security grounds starting after fiscal year 2009, superseding a provision that would have delayed the President's authority to waive or postpone the aggregate amount of funds appropriated by Congress starting after fiscal year 2011 (Section 356). The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—no; Vice Chairman Bond—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—no; Senator Coburn—no; Senator Risch—no.

On July 16, 2009, by a vote of 10 ayes to 5 noes, the Committee adopted an amendment by Senator Feingold to establish a commission on foreign intelligence and information (Title VI). The votes in person or by proxy were as follows: Chairman Feinstein—aye; Sen-

ator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Hatch—no; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—no; Senator Coburn—aye; Senator Risch—no.

On July 16, 2009, by a vote of 14 ayes to 1 no, the Committee adopted an amendment by Senator Feingold to amend the National Security Act of 1947 by requiring that the congressional intelligence committees be provided with the legal authorities under which all covert action and all other intelligence activities are or were conducted (Section 333). The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—aye; Senator Coburn—aye; Senator Risch aye.

On July 16, 2009, by a voice vote, the Committee adopted an amendment by Senator Coburn, as amended by Chairman Feinstein, concerning reports on national security threats posed by Guantanamo Bay detainees (Section 337). The second degree amendment by Chairman Feinstein was adopted by a vote of 9 ayes and 6 noes. The votes in person or by proxy were as follows: Chairman Feinstein—aye; Senator Rockefeller—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Hatch—no; Senator Snowe—aye; Senator Chambliss—no; Senator Burr—no; Senator Coburn—no; Senator Risch—no. The amendment was further amended by unanimous consent.

On July 16, 2009, by a voice vote, the Committee agreed to an amendment by Senator Hatch to establish an awards program for certain exceptional Intelligence Community officers that is further described in the classified annex.

On July 16, 2009, by a voice vote, the Committee agreed to an amendment offered by Senator Chambliss on behalf of Senator Hatch concerning classified activities that are further described in the classified annex.

#### ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to this legislation. On July 21, 2009, the Committee transmitted this bill to the Congressional Budget Office and requested it to conduct an estimate of the costs incurred in carrying out its 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.

ADDITIONAL VIEWS OF VICE CHAIRMAN BOND AND SENATORS HATCH, CHAMBLISS, BURR, COBURN, AND RISCH

For the first time in several years, the Committee has successfully voted out a relatively clean bill that should pass muster with the House and Senate and be signed into law by the President. We attribute much of this success to the leadership of our Chairman, Senator Dianne Feinstein, who worked with all of the Members of the Committee to fashion a bipartisan bill.

GOOD GOVERNMENT PROVISIONS

We are pleased that our bill contains a number of good government provisions that we have been developing over the past several years. These provisions will improve the efficiency and accountability of the Intelligence Community and provide the Director of National Intelligence (DNI) with some additional tools to better perform his duties under the National Security Act of 1947.

A number of these good government provisions relate to the Intelligence Community's budgetary and acquisition processes. Sections 323 and 324 will operate together to address the problem of cost overruns in major system acquisitions by the Intelligence Community. These provisions were modeled on the Nunn-McCurdy provision in title 10 of the United States Code. They encourage greater DNI involvement in the acquisition process and enable the congressional intelligence committees to perform more effective and timely oversight of cost increases.

Section 321 requires the DNI to conduct initial and subsequent vulnerability assessments for any major system, and its items of supply, that is included in the National Intelligence Program (NIP). Such assessments will ensure that any vulnerabilities or risks associated with a particular system are identified and resolved at the earliest possible stage.

Section 325 requires the DNI, with the concurrence of the Office of Management and Budget, to provide the congressional intelligence committees with a future year intelligence plan and a long-term budget projection each fiscal year beginning with the budget for fiscal year 2011. These important planning tools will enable the DNI and the congressional intelligence committees to "look over the horizon" and resolve significant budgetary issues before they become problematic.

Section 322 requires the DNI to create a comprehensive business enterprise architecture that will define all Intelligence Community business systems. This architecture will incorporate Intelligence Community financial, personnel, procurement, acquisition, logistics, and planning systems into one interoperable and modernized system.

Vice Chairman Bond sponsored a new provision this year, Section 359, which is intended to help the Intelligence Community cor-

rect several long-standing management deficiencies, known as “material weaknesses.” These material weaknesses have contributed to the inability of certain Intelligence Community agencies to pass an independent financial audit. Section 359 addresses this problem by requiring the agency heads for the Central Intelligence Agency (CIA), Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and National Security Agency to identify the specific senior intelligence management officials within their respective agencies who are responsible for correcting applicable long-standing material weaknesses.

Section 305 continues the theme of encouraging good government. This section directs the DNI to conduct annual personnel level assessments of each element of the Intelligence Community that capture the number and costs of personnel, including contractors, for that element. These assessments will aid both the DNI and the congressional intelligence committees in the exercise of their respective responsibilities on personnel funding issues.

Finally, Section 401 provides the DNI with the authority to conduct accountability reviews of elements and personnel of the Intelligence Community in relation to their significant failures or deficiencies. This section will encourage Intelligence Community elements to address their own internal failures or deficiencies—something they at times have been reluctant to do before now. In the event that they are reluctant or unable to do so, this provision gives the DNI the authority he needs to conduct his own reviews.

We are confident that these good government measures will lead to a stronger, more efficient, and more effective Intelligence Community. Major systems acquisition is an important issue for our warfighters and intelligence collectors, especially as technological capabilities evolve. It is also essential that the Intelligence Community has sufficient and appropriate personnel to do the demanding jobs that are required to keep our nation safe and defeat our enemies.

#### CLASSIFIED INFORMATION

We have always been strong proponents of protecting classified information. Some might find it strange, then, that Vice Chairman Bond sponsored, and we all supported, an amendment requiring the Director of the CIA to make publicly available an unclassified version of four classified documents assessing the information obtained from certain high-value terrorists.

We believe this amendment, Section 427, was necessary in light of the Administration’s recent declassification and publication of numerous documents about the CIA’s detention and interrogation program. At the time, we objected to the release of these documents because it would give our enemies valuable insights into the types of limitations we impose on our intelligence collectors and allow terrorists to improve their interrogation resistance tactics. That damage has now been done.

Unfortunately, the released documents, selectively chosen and selectively redacted, do not provide the American public with any objective perspective on the value of the information obtained from these high-value detainees. Indeed, with one highly sensitive document, the Administration declassified virtually the entire memo,

except for those paragraphs in which the value of the intelligence obtained was discussed. By requiring the Director of the CIA to provide an unclassified version of these four documents to the public, the American people can make their own assessment of the value of the information obtained from these high-value terrorists.

Let us be clear about what Section 427 does not do: unlike the Administration's recent declassification of highly sensitive detention and interrogation documents, Section 427 does not require the declassification of these four documents. Rather, it requires only the release of an unclassified version prepared by the Central Intelligence Agency. We have reviewed each of the documents covered by this amendment. By limiting Section 427 in this manner, we are confident that no intelligence sources and methods will be disclosed and that there will be no damage to our national security.

#### RELEASE OR TRANSFER OF DETAINEES

Beginning during the Bush Administration and continuing under the current Administration, hundreds of detainees from the Naval Detention Facility at Guantanamo Bay, Cuba (GTMO) have been released or transferred to other countries. Unfortunately, many of these released individuals remain a threat to the United States and its interests. According to information released by the Department of Defense in March of this year, the recidivism rate for these former detainees was more than 14 percent. It is now judged to be even higher. Yet, not one of the threat assessments on these detainees was provided to the congressional intelligence committees prior to their release. This is unacceptable.

In May 2009, the Committee learned that of the 60 detainees at GTMO who have been judged by the current and previous Administrations to be eligible for release or transfer, the Defense Intelligence Agency recommended that 25 continue to be held, due to the threat they posed. Five of those 25 were assessed to "pose the most significant threat of reengagement in serious acts of terrorism." Congress should not be placed in the position of not knowing whether dangerous individuals are being released who may threaten our homeland again.

Senator Coburn offered an amendment that would have solved this problem by requiring the DNI to report to the congressional intelligence committees at least 30 days prior to the release or transfer of any GTMO detainee with an assessment of the detainee's suitability for release or transfer. When his amendment was replaced with a second degree amendment, this useful congressional oversight tool was lost. In its place, Section 337 requires a less timely quarterly report from the DNI that assesses the suitability for release or transfer of detainees previously released or transferred, or to be released or transferred from GTMO. It is conceivable that this formulation could result in certain detainees being transferred or released prior to congressional review of threat assessment information. Also lost as a result of the second degree amendment was a provision that would have allowed the American people to be told when a detainee was released or transferred in spite of a negative threat assessment. We find it ironic, and highly disturbing, that the American people can know when a sex offender



resides in the community, but cannot be told when a former detainee moves in down the street.

#### CONGRESSIONAL NOTIFICATION

Section 332, which we opposed, modifies the current balance in the National Security Act with respect to the congressional notification procedures. It imposes new requirements when the Executive branch determines that disclosure to less than the full membership of the Committee is appropriate. Section 332 requires that, in those cases, the Executive branch must provide the “main features” of the program to the entire membership of the intelligence committees. Although Members who supported this amendment made it clear that they would defer to the Administration’s determination of what “main features” to provide, we are concerned that in the future we may face a circumstance similar to one in which we find ourselves today—where the Administration met the requirements of the National Security Act, but for reasons of political expediency, is nonetheless accused of not fully informing Congress. Closed door assurances will be of small consolation to future CIA employees accused of not adequately providing the “main features.” For this reason, while this general notice requirement is significantly less controversial than its predecessors, we believe this requirement will unnecessarily increase the tension between the Legislative and Executive branches over information access.

We also opposed the adoption of Section 331 because it appears to be little more than legislative surplusage. Section 331 states that “there shall be no exception to the requirements to inform the congressional intelligence committees of all intelligence activities and covert action.” The Select Committee on Intelligence expects the Intelligence Community to comply with the congressional notification procedures in the National Security Act and keep it “fully and currently informed” of all covert actions and intelligence activities. As long as further substantive changes are not made to congressional notification requirements, including Gang of Eight provisions, the addition of this “no exception” clause to the general congressional oversight provision should have little, if any, practical impact on the interpretation of the notification procedures.

CHRISTOPHER “KIT” BOND.  
ORRIN G. HATCH.  
SAXBY CHAMBLISS.  
RICHARD BURR.  
TOM COBURN.  
JAMES E. RISCH.

## ADDITIONAL VIEWS OF SENATORS ROCKEFELLER AND SNOWE

Title V of the National Security Act of 1947 requires the President to ensure that the congressional intelligence committees are kept “fully and currently informed” of the intelligence activities of the United States, including any significant anticipated intelligence activity. For years, we have been very concerned about the way in which the Executive branch has interpreted this obligation. Rather than briefing the full Committee, the Executive branch has restricted briefings about certain classified programs to the Chairman and Vice Chairman of the Committee and the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence.

This is not an academic issue; it is an issue of how our democracy makes critical and secret national security decisions. Without the intelligence committees’ meaningful independent review and oversight—the very reason for the committees’ existence—intelligence programs are susceptible to both mistakes and illegitimacy. This is the case regardless of which party is in the White House or which party has a majority in Congress.

With this in mind, we supported an amendment to the authorization bill that will establish in statute new requirements regarding notification. This amendment is not a wholesale change to the long-standing law of congressional notifications, and it does not eliminate the “Gang of Eight” notification process regarding covert actions, which many of us believe can serve an important purpose for quick and timely notifications on extraordinarily sensitive covert actions.

Instead, the amendment seeks to improve the notification processes that have existed for years. The amendment will require that whenever the DNI or an intelligence agency chief chooses to brief less than the full committee on an intelligence activity or invokes the “Gang of Eight” provision regarding covert action, he or she must (1) notify the full committee of that fact and (2) provide a description of the “main features” of the activity or covert action in question. The amendment enforces these requirements by prohibiting funds for intelligence activities and covert actions that are not so notified.

This amendment has had bipartisan support for many years. In fact, a bipartisan majority of the Senate Intelligence Committee has adopted this amendment in fiscal years 2007, 2008, 2009, and 2010. In three different Congresses and under two different Administrations, this Committee has on four occasions expressed its view regarding congressional notifications in cases when the full Committee is not briefed. It should be clear that year in and year out, this Committee holds the same consistent opinion on this funda-

mental issue of Congressional oversight—no matter who is in power at either end of Pennsylvania Avenue.

This amendment favors no particular party and no particular branch of government; it simply addresses an important concern. The Committee's oversight of the Executive branch's intelligence activities should not be adversarial; it should be a true, trusted and confidential partnership aimed exclusively at improving our nation's collection and analysis capabilities, and ensuring the effectiveness and legitimacy of our covert action programs.

Together with the other congressional notification amendments that the Committee has accepted in the fiscal year 2010 authorization bill, this amendment will strengthen our constructive oversight relationship with the Executive branch and the intelligence community.

JOHN D. ROCKEFELLER IV.  
OLYMPIA J. SNOWE.

## ADDITIONAL VIEWS OF SENATOR FEINGOLD

The Fiscal Year 2010 Intelligence Authorization bill includes an amendment I offered to establish an independent commission to significantly reform and improve our intelligence capabilities. The amendment, which is similar to the Feingold-Hagel amendment of last year and which was again approved on a bipartisan basis, addresses structural problems in our government that prevent global coverage and perpetuate gaps in our ability to anticipate terrorist as well as other threats and crises before they appear. For example, the 9/11 Commission recommended that the “U.S. government must identify and prioritize actual or potential terrorist sanctuaries.” Yet, as the Director of the National Counterterrorism Center has testified, “much of the information about the instability that can lead to safe havens or ideological radicalization comes not from covert collection but from open collection, best done by Foreign Service Officers.” The commission established by the amendment would thus focus on the critical reform of integrating the country’s intelligence capabilities with the open gathering and reporting of information by other elements of the United States Government, particularly the State Department, thereby strengthening our overall collection, reporting and analytical capabilities.

The Committee also approved my amendment, cosponsored by Committee Vice Chairman Bond and Senator Wyden, requiring the president to submit an unclassified top-line budget request for the National Intelligence Program. This reform makes possible a recommendation of the 9/11 Commission to improve oversight by passing a separate intelligence appropriations bill and provides for greater transparency and accountability for intelligence spending. It is my view that the Senate should also implement another one of the Commission’s recommendations—granting appropriations authorities to the Senate Intelligence Committee—by passing the bipartisan S. Res. 164.

The Committee approved an amendment I offered requiring that the congressional intelligence committees be provided with the legal authorities under which all covert action and other intelligence activities are or were conducted. This requirement, which will allow the committees to review the opinions of the Department of Justice’s Office of Legal Counsel (OLC), those of the General Counsels of entities of the Intelligence Community, and other legal bases for intelligence activities, follows years of efforts by the Committee to obtain legal justifications for various intelligence programs. The Fiscal Year 2007, 2008, 2009 and 2010 Intelligence Authorization bills required that the Committee be provided all guidelines on the application of the Detainee Treatment Act to the detention and interrogation activities of the Intelligence Community, including legal opinions of the Department of Justice on the matter. The Committee also repeatedly requested Department of Jus-

tice legal opinions that supported the warrantless wiretapping program, the actual text of which the Committee described, in its report accompanying the FISA Amendments Act (FAA), as “important for obtaining a complete understanding of the program.” The frequent challenges faced by the Committee, as well as the highly selective nature of executive branch cooperation (opinions related to the warrantless wiretapping program were only made available nine days before the Committee’s mark-up of the FAA) require a clear statutory obligation to provide legal opinions as a matter of course.

The bill also includes a number of important efforts to improve oversight of current intelligence activities. An amendment offered by Chairman Feinstein that I co-sponsored requires that the Committee be provided critical documents related to cybersecurity activities, including the legal justifications for those activities, any certifications of legality, privacy impact assessments, and a plan for independent audits. The bill also limits funding for elements of the Comprehensive Cybersecurity Initiative pending receipt of documents related to the privacy of Americans and to the legal basis for the Initiative, including any analysis by the OLC under the current administration. This follows an amendment I included in last year’s bill to limit funding until the Committee received other critical information related to the Initiative. Finally, the bill withholds funding for a different intelligence program until members’ committee staff have access to the program. Limited staff access impedes meaningful oversight and I have repeatedly registered my concerns about the persistence of this problem.

Efforts in recent years to improve congressional oversight have also included addressing the abuse of the so-called “Gang of Eight” provision of the National Security Act, most notably in the cases of the previous administration’s detention and interrogation and warrantless wiretapping programs. The bill includes an amendment ensuring that all members of the Committee receive basic information about matters only briefed to the Chairman and Vice Chairman. While I supported the amendment, I am concerned that, unless all members of the Committee are fully notified of all intelligence activities, including covert action, effective oversight of operational, policy, budgetary and legal aspects of those activities will not be possible. It is therefore my position that the “Gang of Eight” provision should be eliminated entirely.

It is my position that legislative action is still required in the area of interrogation, detention and rendition. While I applauded President Obama’s swift, unilateral action to end the CIA’s detention and interrogation program, Executive Orders can be withdrawn, and the previous administration even asserted the authority to do so secretly. Moreover, the overwhelming legal, moral and policy grounds for prohibiting torture and secret detention transcend changes in administration and require clear statutory language to bind future presidents as well.

Greater statutory clarity is also needed in the area of rendition. Under the January 22, 2009 Executive Order on detention and the interrogation, the CIA has the authority to temporarily detain individuals and transfer them to foreign countries. While the law prohibits transfer if a detainee is likely to be tortured, it does not spe-

cifically prohibit the CIA from knowingly transferring a detainee to extended incommunicado detention or indefinite detention without charge. Yet State Department human rights reports have made clear the direct connection between indefinite, incommunicado detention and torture. Moreover, our government has condemned such detention by other countries around the world, regardless of whether the detained individuals were subjected to physical mistreatment. New legislation is therefore required to ensure that any CIA renditions are consistent, not only with our legal obligations, but with U.S. policy and with our values.

The bill includes two amendments offered by Senator Wyden that I co-sponsored, ensuring access to the Intelligence Community by the Government Accountability Office, and strengthening the role of the Public Interest Declassification Board. These provisions further accountability and transparency.

Finally, I am concerned about a provision of the bill creating an exemption from the Freedom of Information Act for certain information related to terrorist watchlisting. It is not yet clear that this new statutory exemption is needed and I will continue to work with the Committee and with the ODNI on this matter.

RUSSELL D. FEINGOLD.

○