

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR  
2006

---

SEPTEMBER 29, 2005.—Ordered to be printed

---

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

R E P O R T

[To accompany S. 1803]

The Select Committee on Intelligence, to which was referred the bill (S. 1803) having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

The Select Committee on Intelligence (SSCI or Committee), having considered the original bill (S. 1803), to authorize appropriations for fiscal year 2006 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports an original bill without amendment favorably thereon and recommends that the bill do pass.

CLASSIFIED SUPPLEMENT TO THE COMMITTEE REPORT

The classified nature of United States intelligence activities precludes disclosure by the Committee of details of its budgetary recommendations in this Report. The Committee has prepared a classified supplement to this Report that contains (a) the Classified Annex to this Report and (b) the classified Schedule of Authorizations. The Schedule of Authorizations is incorporated by reference in the Act and has the same legal status as public law. The Classified Annex to this Report explains the full scope and intent of the Committee's actions in the classified Schedule of Authorizations. The Classified Annex has also been incorporated by reference in Section 103. As such, the Intelligence Community is required to comply with any directions or requirements contained therein as it would any other statutory requirement.

The classified supplement to the Report is available for review by any Member of the Senate, subject to the provisions of Senate Res-

olution 400 of the 94th Congress, as amended by Senate Resolution 445 of the 108th Congress.

The classified supplement is made available to the Committees on Appropriations of the Senate and the House of Representatives, to the Permanent Select Committee on Intelligence of the House of Representatives, and to the President. The President shall provide for appropriate distribution within the Executive Branch.

#### SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the Intelligence Authorization Act for Fiscal Year 2006, as reported herein. Following the section-by-section analysis and explanation there are Committee comments on other matters. The report also includes additional views offered by Committee Members regarding this legislation and other matters.

#### TITLE I—INTELLIGENCE ACTIVITIES

##### *Section 101. Authorization of appropriations*

Section 101 lists the United States government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for fiscal year 2006.

##### *Section 102. Classified schedule of authorizations*

Section 102 makes clear that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities and the applicable personnel ceilings covered under this title for fiscal year 2006 are contained in a classified Schedule of Authorizations. The 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. Incorporation of classified annex*

Section 103 incorporates into law the Classified Annex to this Report. Unless otherwise specifically stated, the amounts authorized in the Classified Annex are not in addition to amounts authorized to be appropriated by other provisions of the Act or by the classified Schedule of Authorizations.

The Committee has taken the step of incorporating the Classified Annex because the Executive Branch has refused to treat with equal weight the language in the classified annexes and the text of recent authorization acts and their accompanying classified schedules of authorizations. This Committee, and Congress, will not permit the Executive Branch to ignore the clear instructions of Congress merely because the directives are contained, by necessity of classification, in an annex accompanying the report associated with intelligence authorizing legislation. The Committee directs the Executive Branch to comply fully with any directed transfers, temporary limitations on use (fences), or other limitations or instructions contained in the Classified Annex to this Report.

##### *Section 104. Personnel ceiling adjustments*

Section 104 authorizes the Director of National Intelligence (DNI), with the approval of the Director of the Office of Manage-

ment and Budget (OMB), in fiscal year 2006 to authorize employment of civilian personnel in excess of the personnel ceilings applicable to the elements of the Intelligence Community under Section 102 by an amount not to exceed 2 percent of the total of the ceilings applicable under Section 102. The DNI may exercise this authority only if necessary to the performance of important intelligence functions. Any exercise of this authority must be reported to the intelligence committees of the Congress.

*Section 105. Intelligence Community Management Account*

Section 105 authorizes appropriations for the Intelligence Community Management Account (CMA) of the DNI and sets the personnel end-strength for the Intelligence Community Management Staff for fiscal year 2006.

Subsection (a) authorizes appropriations of \$1,014,362,000 for fiscal year 2006 for the activities of the CMA of the DNI. Subsection (a) also authorizes funds identified for advanced research and development to remain available for two years.

Subsection (b) authorizes 882 full-time personnel for elements within the CMA for fiscal year 2006 and provides that such personnel may be permanent employees of the CMA element or detailed from other elements of the United States government.

Subsection (c) authorizes additional appropriations and personnel for the CMA as specified in the classified Schedule of Authorizations and permits the additional funding for research and development to remain available through September 30, 2007.

Subsection (d) requires that, except as provided in Section 113 of the National Security Act of 1947, personnel from another element of the United States government shall be detailed to an element of the CMA on a reimbursable basis, except that for temporary functions such personnel may be detailed on a non-reimbursable basis for periods of less than one year.

Subsection (e) authorizes \$17,000,000 of the amount authorized in subsection (a) to be made available for the National Drug Intelligence Center (NDIC). Subsection (e) requires the DNI to transfer these funds to the Department of Justice (DoJ) to be used for NDIC activities under the authority of the Attorney General, and subject to Section 104A(e)(1) of the National Security Act of 1947, as amended by Section 421(b)(1) of this Act.

*Section 106. Incorporation of reporting requirements*

Section 106 incorporates into the Act by reference each requirement to submit a report contained in the joint explanatory statement to accompany the conference report or in the classified annex accompanying the conference report.

*Section 107. Response of intelligence community to requests from Congress for intelligence documents and information*

Section 107 provides for certain procedural requirements related to the ability of Congress to gain access, through the intelligence committees and other committees of jurisdiction, to intelligence reports, assessments, estimates, legal opinions, and other intelligence information. The provision states that elements of the Intelligence Community must provide to the intelligence committees any intelligence documents or information requested by the Chairman or

Vice Chairman (or Ranking Minority Member) of such committees. The statutory requirement applies only to existing intelligence documents and information and would not apply to requests to generate new intelligence assessments, reports, estimates, legal opinions, or other information.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND  
DISABILITY SYSTEM

*Section 201. Authorization of appropriations*

Section 201 authorizes appropriations in the amount of \$244,600,000 for fiscal year 2006 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—INTELLIGENCE AND GENERAL INTELLIGENCE COMMUNITY  
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 such compensation or benefits authorized by law.

*Section 302. Restriction on conduct of intelligence activities*

Section 302 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

*Section 303. Clarification of definition of intelligence community under the National Security Act of 1947*

Section 303 amends Section 3(4)(L) of the National Security Act of 1947 (50 U.S.C. 401a(4)(L)) to permit the designation as “elements of the intelligence community” of other elements of departments and agencies of the United States government not listed in Section 3(4). Section 3(4)(L) is redesignated as Section 3(4)(M) by Section 441(d) of this Act.

*Section 304. Delegation of authority for travel on common carriers for intelligence collection personnel*

Section 116 of the National Security Act of 1947 (50 U.S.C. 404k) allows the DNI to authorize travel on any common carrier when it is consistent with Intelligence Community mission requirements or, more specifically, is required for cover purposes, operational needs, or other exceptional circumstances. As presently written, the DNI may only delegate this authority to the Principal Deputy DNI or, with respect to Central Intelligence Agency (CIA) employees, to the Director of the CIA.

Section 304 of this bill provides that the DNI may delegate the authority in Section 116 of the National Security Act of 1947 to the head of any element of the Intelligence Community. This expansion is consistent with the view of the Committee that the DNI should be able to delegate authority throughout the Intelligence Commu-

nity when such delegation serves the overall interests of the Community.

Section 304 also provides that the head of an Intelligence Community element to whom travel authority has been delegated is also empowered to delegate the authority to senior officials of the element as specified in guidelines issued by the DNI. This allows for administrative flexibility, consistent with the guidance of the DNI, for the entire Community. To facilitate Congressional oversight, the DNI shall submit the guidelines to the intelligence committees of the Congress.

*Section 305. Modification of availability of funds for different intelligence activities*

Section 305 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 and Terrorism Prevention Act of 2004 (Pub. L. No. 108–458 (Dec. 17, 2004)) (governing the transfer and reprogramming by the DNI of certain intelligence funding). In particular, this conforming amendment replaces the “unforeseen requirements” standard in Section 504(a)(3)(B) with a clearer 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 would be 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 306. Retention and use of amounts paid as debts to elements of the intelligence community*

Section 306 adds a new Section 1103 to the National Security Act of 1947, authorizing Intelligence Community elements to accept, retain, and—for certain purposes—use amounts received from private parties as repayment of debts owed to such element.

Each year some property purchased with appropriated funds is damaged beyond use or is lost through the negligence of a private party or an employee of the Intelligence Community. The damaged or lost property may have been used to support wartime activities or other national intelligence missions and, thus, waiting for the next annual appropriation cycle for additional funds to repair or replace the property inhibits the Intelligence Community’s ability to quickly and efficiently support the war fighter and other national intelligence missions.

Section 306 addresses this shortcoming by authorizing elements of the Intelligence Community to accept and retain reimbursement, outside of the annual appropriations cycle, from a private party, including a Federal employee, who has been found to have neg-

ligerly lost or damaged property. As a result, elements of the Intelligence Community will be able to expeditiously repair or replace lost or damaged property without waiting for the next appropriation cycle. Similarly, this new section also authorizes elements of the Intelligence Community to retain funds paid by Intelligence Community employees or former employees as repayment of a default on the terms and conditions of scholarship, fellowship, or other educational assistance provided by the Community to the employee. The section authorizes crediting payments only to the current appropriation account related to the debt and limits the subsequent use of the funds.

*Section 307. Pilot program on disclosure of records under the Privacy Act relating to certain intelligence activities*

As a result of reporting requirements in the Intelligence Authorization Act for Fiscal Year 2004 (Pub. L. No. 108-177 (Dec. 13, 2003)) intended to improve information access across the Intelligence Community and the Federal government, the Intelligence Community, Department of Defense (DoD), Department of Homeland Security, and Federal law enforcement agencies formed the Information Sharing Working Group (ISWG) to, inter alia, identify impediments to information access in existing laws and in Intelligence Community and DoD policies. The ISWG issued its report in December 2004.

In the report, the ISWG noted that certain provisions of the Privacy Act could prevent the sharing of intelligence information within the Executive Branch. Generally, the Privacy Act (5 U.S.C. 552a) precludes the dissemination of information regarding U.S. persons stored within a system of records maintained by the United States government without the consent of that individual. There are, however, twelve exceptions to this general rule. For example, one exception permits the sharing of information to support a civil or criminal law enforcement activity under certain prescribed circumstances. There is no exception permitting Intelligence Community elements and other United States government agencies to share foreign intelligence or counterintelligence information (including information concerning international terrorism or proliferation of weapons of mass destruction) between or with elements of the Intelligence Community.

To address this shortcoming, Section 307 creates a pilot program to study a narrow intelligence exception to the Privacy Act. Specifically, the provision allows transfers under three circumstances. First, the provision permits elements of the Intelligence Community, including their parent departments and agencies, to share with other elements of the Intelligence Community, and their parent departments and agencies, information covered by the Privacy Act when that information is relevant to a lawful and authorized foreign intelligence or counterintelligence activity. Second, the provision permits the head of an element of the Intelligence Community to request in writing Privacy Act records relevant to a lawful and authorized activity of that element to protect against international terrorism or the proliferation of weapons of mass destruction from another United States government agency with similar responsibilities related to protection against international terrorism and proliferation. Third, the provision authorizes heads of non-In-

telligence Community agencies with responsibilities to protect against international terrorism or the proliferation of weapons of mass destruction to share Privacy Act records with an element of the Intelligence Community if the record constitutes “terrorism information” (as defined in Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108–458 (Dec. 17, 2004)) or information concerning the proliferation of weapons of mass destruction, if the receiving element of the Intelligence Community is lawfully authorized to collect or analyze the information to protect against international terrorism or proliferation. When necessary to determine whether a record held by a non-Intelligence Community agency constitutes terrorism information or information concerning the proliferation of weapons of mass destruction, the head of such agency may consult the DNI or the Attorney General. Section 307 also extends to the pilot program an exemption from certain records access and disclosure accounting requirements. In order to protect intelligence sources and methods from unauthorized disclosure, this exemption is identical to the exemption extended to the DNI under Section 416 of this Act.

Section 307 facilitates the sharing only of intelligence information already lawfully collected and maintained within United States government record systems and relevant to a lawful and authorized foreign intelligence or counterintelligence activity (with a particular focus on sharing by non-Intelligence Community elements on information concerning international terrorism and the proliferation of weapons of mass destruction). The provision expressly states that the new authority does not permit the collection or retention of foreign intelligence or counterintelligence information not otherwise authorized by law.

To ensure that the exception to the Privacy Act permits necessary sharing of critical foreign intelligence and counterintelligence information while providing appropriate protections for the privacy and civil liberties of U.S. persons, Section 307 establishes a four-year pilot program. The exception to the Privacy Act will expire on December 31, 2009, unless renewed. In the interim, the DNI and the Attorney General, in consultation with the Privacy and Civil Liberties Oversight Board, are required to submit to the intelligence committees an annual report on the status and implementation of the pilot program. On June 31, 2009, the DNI and the Attorney General, in coordination with the Privacy and Civil Liberties Oversight Board, will submit a final report to the intelligence committees, including any recommendations regarding continued authorization of the exception. Additionally, the Privacy and Civil Liberties Oversight Board will submit to the Congressional intelligence committees a separate report providing the Board’s advice and counsel on the development and implementation of the authorities provided under this Section.

*Section 308. Extension to intelligence community of authority to delete information about receipt and disposition of foreign gifts and decorations*

Current law requires that certain Federal “employees”—a term that generally applies to all officials and personnel of the Intelligence Community and certain contractors, spouses, dependents, and others—file reports with their “employing” agency regarding

the receipt of gifts or “decorations” from foreign governments. See 5 U.S.C. 7342. Following compilation of these reports, the “employing” agency is required to annually file with the Secretary of State detailed information about the receipt of foreign gifts and decorations reported by its employees, including the source of the gift. See 5 U.S.C. 7342(f). The Secretary of State is then required to publish a comprehensive list of the agency reports in the Federal Register. See *id.* With respect to the activities of the Intelligence Community, the public disclosure of such gifts or decorations in the Federal Register has the potential to compromise intelligence sources (e.g., the confirmation of an intelligence relationship with a foreign government) and could undermine national security. Recognizing this potential concern, the Director of Central Intelligence (DCI) was granted a limited exemption from reporting certain specified information about such foreign gifts or decorations where the publication of the information could adversely affect United States intelligence sources. See Pub. L. No. 95–105, Sec. 515(a) (Aug. 17, 1977). Section 1079 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458 (Dec. 17, 2004) (“Intelligence Reform Act”), extended a similar exemption to the DNI (in addition to amending the existing exemption to apply to the Director of the CIA).

Section 308 amends existing law to provide 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 the Director of the CIA. The national security concerns that prompted the initial DCI exemption, and the more recent exemptions for the DNI and Director of the CIA, apply with equal weight to other Intelligence Community elements—the publication of certain information relating to foreign gifts or decorations provided to employees of all Intelligence Community agencies could adversely affect United States intelligence sources. Section 308 provides the exemption necessary to protect national security, but mandates that the information not provided to the Secretary of State be provided to the DNI to ensure continued independent oversight of the receipt by Intelligence Community “employees” of foreign gifts or decorations.

*Section 309. Availability of funds for travel and transportation of personal effects, household goods, and automobiles*

Section 309 provides the CIA and the Office of the DNI the same authority that is granted to the Department of State by Section 2677 of Title 22, United States Code, when travel and transportation authorized by valid travel orders begins in one fiscal year, but may not be completed during that same fiscal year. The Committee believes this authority will relieve the administrative burden of charging the eligible costs to two fiscal years’ appropriations and adjusting associated accounts.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE  
COMMUNITY

## Subtitle A—Office of the Director of National Intelligence

*Section 401. Additional authorities of the Director of National Intelligence on intelligence information sharing*

Section 401 amends the National Security Act of 1947 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) of the National Security Act of 1947 authorizes the DNI to provide to a receiving agency or component—for that agency or component to accept and use—funds that have been authorized and appropriated to address intelligence information access or sharing needs. In the alternative, the DNI may provide to a receiving agency necessary or associated services and equipment procured with funds from the National Intelligence Program. The new Section 102A(g)(1)(H) of the National Security Act of 1947 also grants the DNI the 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 the authority, the 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 new DNI authorities are similar to authority granted to the National Geospatial-Intelligence Agency (NGA) with respect to imagery and imagery-related systems. See Section 105(b)(2)(D)(ii) of the National Security Act of 1947 (50 U.S.C. 403–5).

*Section 402. Modification of limitation on delegation by the Director of National Intelligence of the protection of intelligence sources and methods*

Section 402 amends the National Security Act of 1947 to modify the limitation on delegation by the DNI of the authority to protect intelligence sources and methods from unauthorized disclosure. The provision permits the DNI to delegate the authority to the Deputy Directors of National Intelligence or the Chief Information Officer of the Intelligence Community. A previous provision in the National Security Act of 1947 had vested the power to protect sources and methods in the DCI, but did not constrain further delegation of the authority.

*Section 403. Authority of the Director of National Intelligence to manage access to human intelligence information*

Section 403 provides the DNI with the authority to ensure the dissemination of intelligence information collected through human sources, including the underlying operational data necessary to understand that reporting, to appropriately cleared analysts or other intelligence officers throughout the Intelligence Community. Recent intelligence failure—particularly related to pre-war intelligence assessments on Iraq—have demonstrated the importance of rebuilding and improving the nation's human intelligence capabilities.

While the Intelligence Community is making some progress in this regard, a great deal remains to be done, particularly in the area of access to intelligence gathered through human intelligence operations.

The Committee's review of the Intelligence Community's pre-war assessments on Iraq highlighted the impact of unnecessary restrictions on access by intelligence analysts to human intelligence information. In its Report of the Select Committee on Intelligence on the U.S. Intelligence Community's Pre-War Intelligence Assessments on Iraq, the Committee concluded that the Intelligence Community's failure to provide cleared analysts with a legitimate need-to-know broader access to human intelligence reporting, including the operational data underlying that reporting, contributed to the flawed intelligence assessments on Iraq's weapons of mass destruction programs. Access to this data—controlled by the agencies that collected the information—would have provided analysts with a better understanding of the reliability of the sources of the reporting, as well as other significant intelligence information required for their work.

The Intelligence Reform Act provides the DNI with a number of tools to foster greater information access within the Community. Section 403 builds on these tools by providing the DNI with the specific authority to ensure analysts and other Intelligence Community officers are provided with improved access to human intelligence reporting, consistent with the DNI's determinations regarding the protection of intelligence sources and methods. Although the Committee expects that individual elements will continue to retain human intelligence operational data, access decisions will be made by the DNI as a neutral arbiter of need-to-know. No longer will these access decisions be left to individual agencies with a parochial—and understandable—desire to protect sources at all costs. Access to human intelligence reporting, and underlying operational reporting, must be balanced against real threats to sources and methods. Under Section 403, the Committee expects the DNI to perform the necessary balancing. Section 403 also provides the DNI with full and regular access to the information necessary to “manage and direct . . . the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community.” See Section 102A(f)(1)(A)(ii) of the National Security Act of 1947 (50 U.S.C. 403–1(f)(1)(A)(ii)).

To effectively implement Section 403, the DNI should standardize security clearance processes across Intelligence Community elements to resolve issues that have hampered information access in the past. The Committee does not believe that working in a particular agency makes one Intelligence Community officer inherently more trustworthy than a counterpart with the same security clearance and a legitimate “need-to-know” at another element. Resolution of disparate clearance standards and processes, however, should provide Intelligence Community elements with an additional degree of comfort that, while information from sources for which those agencies are responsible has received greater distribution, the recipients of that information are appropriately cleared consistent with DNI standards. Based on the authorities provided to the DNI in the Intelligence Reform Act and this section, the Committee is confident that the DNI can implement the protections

necessary for intelligence sources and methods, while making human intelligence information more readily available to appropriately cleared intelligence officers who need the information for the conduct of their duties.

*Section 404. Additional administrative authority of the Director of National Intelligence*

From an organizational standpoint, the DNI should be able to rapidly focus the Intelligence Community on a particular intelligence issue through a coordinated effort that uses all available resources. The ability of the DNI to respond with flexibility and to coordinate the Intelligence Community response to an emerging threat should not depend on the time-sensitive vagaries of the budget cycle and should not be constrained by general limitations found in appropriations law (e.g., 31 U.S.C. 1532) or the annual limitation set forth in the “General Provisions” of the Transportation, Treasury, Housing and Urban Development, the Judiciary, the District of Columbia, and Independent Agencies Appropriations Act. See, e.g., Consolidated Appropriations Act, 2005, Division H—Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, Section 610, Pub. L. No. 108–447 (Dec. 8, 2004); see also, e.g., *In re: Veterans Administration Funding of Federal Executive Boards*, 65 Comp. Gen. 689 (July 1, 1986) (discussing history of prohibition on interagency financing of boards, commissions, councils, committees, or similar groups).

To provide this needed operational and organizational flexibility, Section 404 grants the DNI the authority—notwithstanding certain specified provisions of general appropriations law—to approve interagency financing of national intelligence centers (authorized under Section 119B of the National Security Act of 1947 (50 U.S.C. 404o–2)) and of other boards, commissions, councils, committees, or similar groups established by the DNI (e.g., “mission managers,” as recommended by the Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction (WMD Commission)). Under Section 404, the DNI could authorize the pooling of resources from various Intelligence Community and non-Intelligence Community agencies to finance national intelligence centers or other organizational groupings designed to address identified intelligence matters. Once approved by the DNI, the provision also expressly permits other United States government departments and agencies, including Intelligence Community elements, to fund, or participate in the funding of, the authorized activities.

The Committee recognizes the need for coordinated responses to national security threats and intelligence problems. To better understand how the DNI intends to utilize the authority provided under Section 404, the Committee directs the DNI to provide an annual report—through the end of Fiscal Year 2010—providing details on how this authority has been exercised, what amount of appropriated funds attributable to each interagency contributor has been accessed to finance each national intelligence center or other organizational grouping under this section, and whether the National Intelligence Program or other budget account has been modified to provide specific funding for such national intelligence centers or other organizational groupings or whether funding will continue to be provided under the authority of Section 404.

*Section 405. Clarification of limitation on co-location of the Office of the Director of National Intelligence*

Section 405 clarifies that the ban on co-location of the Office of the DNI with any other Intelligence Community element, which is slated to take effect as of October 1, 2008, applies to the co-location of the headquarters of the Office of the DNI with the headquarters of any Intelligence Community agency or element. This provision provides flexibility to ensure that components of the Office of the DNI may be located in the most appropriate facility or facilities, including co-location with components of Intelligence Community agencies or elements. The Committee is aware that the DNI intends to find a headquarters that is separate and apart from the headquarters of the various Intelligence Community elements, consistent with the expressed intent of Congress.

*Section 406. Additional duties of the Director of Science and Technology of the Office of the Director of National Intelligence*

As part of the restructuring of the nation's intelligence infrastructure in the Intelligence Reform Act, Congress created a Director of Science and Technology within the Office of the DNI. Under the Act, the Director of Science and Technology serves as the DNI's chief representative for science and technology, assisting the DNI in formulating a long-term strategy for scientific advances in the field of intelligence and on the science and technology elements of the intelligence budget. Additionally, the Director of Science and Technology chairs the DNI's Science and Technology Committee—responsible for coordinating advances in intelligence-related research and development.

The House-passed version of the Intelligence Authorization Act for Fiscal Year 2006, H.R. 2475 (109th Congress), contains a provision (Section 304) that further expounds on the role of the Director of Science and Technology. Section 304 in H.R. 2475 would require the Director of Science and Technology to systematically identify the Intelligence Community's most significant challenges requiring technical solutions and to develop options to enhance research and development efforts to meet requirements in a timely manner. Section 304 would also require the DNI to submit to Congress a report detailing the strategy for development and use of technology throughout the Intelligence Community through 2021. The report is to identify the Community's highest priority intelligence gaps that may be resolved by the use of technology; identify goals for advanced research and development; explain how advanced research and development projects funded under the National Intelligence Program address the identified gaps; specify current and projected research and development projects; and provide a plan for incorporating technology from research and development projects into National Intelligence Program acquisition programs.

Section 406 incorporates additional requirements into a provision otherwise similar to Section 304 of H.R. 2475.

The Committee supports the House provision, but also believes that such a provision should make clear that it is the responsibility of the Director of Science and Technology to assist the DNI in ensuring that the Intelligence Community's research and development priorities and projects are consistent with national intelligence requirements; that a priority be placed on addressing iden-

tified deficiencies in the collection, processing, analysis, or dissemination of national intelligence; that the research and development priorities and projects account for program development and acquisition funding constraints; and that such priorities and projects address system requirements from collection to final dissemination.

The Committee further requires the Director of Science and Technology, at the direction of the DNI, to develop and maintain an integrated Technical Standards System for major acquisitions. The Technical Standards System should improve the availability of technical standards for the design, development, and operation of Intelligence Community programs and projects; reduce duplication of effort and improve interoperability within the Intelligence Community, with the private sector, and with international partners; and enhance awareness of standardization in the Intelligence Community. Under this provision, the Director of Science and Technology will develop standards that document uniform engineering and technical requirements for processes, procedures, practices, and methods, including requirements for selection, application, and design criteria of particular items. The Committee encourages the DNI to consult, as appropriate, with the heads of other United States government departments and agencies (e.g., the Secretary of Defense, the Administrator of the National Aeronautics and Space Administration, Secretary of Homeland Security) when developing standards and specifications under this provision.

*Section 407. Appointment and title of Chief Information Officer of the Intelligence Community*

Section 407 converts the position of Chief Information Officer (CIO) of the Intelligence Community from an appointment by the President, by and with the advice and consent of the Senate, to an appointment by the DNI. The provision also expressly designates the position as CIO of the Intelligence Community. The modification to the title of the position of CIO is consistent with the position's overall responsibilities as outlined in Section 103G(b) of the National Security Act of 1947 (50 U.S.C. 403-3g(b)).

The creation of a CIO of the Intelligence Community (Section 303 of the Intelligence Authorization Act for Fiscal Year 2005 (Pub. L. No. 108-487 (Dec. 23, 2004)), combined with the budgetary authorities and information technology responsibilities of the DNI (see, e.g., Section 1011 of the Intelligence Reform Act), laid an important foundation for improvements in the information technology infrastructure of the Intelligence Community. The Committee believes that the CIO of the Intelligence Community must provide direction and guidance to all elements of the Intelligence Community to ensure that information technology research and development, security, and acquisition programs support information access throughout the Intelligence Community. The modification to the manner in which the CIO of the Intelligence Community is appointed should not be construed to diminish the authorities or responsibilities of the position.

Under existing law, the President has submitted a nomination for the position of CIO of the Intelligence Community. The Committee will proceed to consider and, as appropriate, act on the nomination. If Senate confirmation precedes conference action on this Act, the Committee will ask the conference to provide that the

amendment proposed in Section 407 not apply until a vacancy in the position of CIO of the Intelligence Community next occurs.

*Section 408. 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 “would be beneficial to improving the operations and effectiveness of the Office of the DNI.” It further provides that the DNI may grant to the Inspector General “any of the duties, responsibilities, and authorities” set forth in the Inspector General Act of 1978. The DNI has now appointed an Inspector General; however, the duties, responsibilities, and authorities of the Inspector General, and his ability to exercise his authorities across all elements of the Community, remain ambiguous.

The DNI and the Intelligence Community need an empowered and effective Inspector General. A strong Inspector General 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, including the manner in which elements of the Community interact with each other in such matters as providing access to information and undertaking joint or cooperative activities. To that end, by way of a proposed new Section 103H of the National Security Act of 1947, Section 408 of this Act establishes an Inspector General for the Intelligence Community.

The office will be established within the Office of the DNI. The Inspector General will keep both the DNI and the intelligence committees fully and currently informed about problems and deficiencies in Intelligence Community programs and operations and the need for corrective actions. The Inspector General will be appointed by the President, with the advice and consent of the Senate, and will report directly to the DNI. To bolster the Inspector General’s independence within the Intelligence Community, the Inspector General may be removed only by the President, who must then communicate the reasons for the Inspector General’s removal to the intelligence committees.

The DNI may prohibit the Inspector General from conducting an investigation, inspection, or audit if the DNI determines that is necessary to protect vital national security interests. If the DNI exercises the authority to prohibit an investigation, the DNI must provide the reasons for taking such action to the intelligence committees within seven days. The Inspector General may, as necessary, provide a response to the intelligence committees regarding the actions of the DNI.

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

The Inspector General 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 Inspector General may request information from any United States government department, agency, or element. Upon receiving such a request from the Inspector General, heads of United States government departments, agencies, and elements, insofar as practicable and not in violation of law or regulation, must provide the requested information to the Inspector General.

The Inspector General must submit semiannual reports to the DNI that include a description of significant problems relating to Intelligence Community programs and operations and to the relationships between Intelligence Community elements. The reports must include a description of Inspector General recommendations and a statement whether corrective action has been completed. Within thirty days of receiving the report from the Inspector General, the DNI must submit each semiannual report to Congress.

The Inspector General must immediately report to the DNI particularly serious or flagrant violations. Within seven days, the DNI must transmit those reports to the intelligence committees, together with any comments. In the event the Inspector General is unable to resolve differences with the DNI, the Inspector General is authorized to report the serious or flagrant violation directly to the intelligence committees. Reports to the intelligence committees are also required with respect to investigations concerning high-ranking Intelligence Community officials.

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 Inspector General. Following a review by the Inspector General to determine the credibility of the complaint or information, the Inspector General must transmit such complaint and information to the DNI. On receiving the complaints or information from the Inspector General (together with the Inspector General’s credibility determination), the DNI must transmit such complaint or information to the intelligence committees. If the Inspector General does not find a complaint or information to be credible, the reporting individual may submit the matter directly to the intelligence 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 Inspector General for the Intelligence Community and an Inspector General for another Intelligence Community element (or a parent department or agency), the Inspectors General must expeditiously resolve who will undertake the investigation, inspection, or audit. The final decision about jurisdiction will, however, be made by the Inspector General for the Intelligence Community. For investigations, inspections, or audits commenced by an Inspector General for an Intelligence Community element prior to the enactment of this Act, the Inspec-

tor General for the Intelligence Community should exercise his authority in a manner that does not disrupt the timely completion of such investigations, inspections, or audits or result in unnecessary duplication of effort. An Inspector General for an Intelligence Community element must share the results of any inspection, investigation, or audit with any other Inspector General, including the Inspector General for the Intelligence Community, who otherwise would have also had jurisdiction over the investigation.

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 409. Leadership and location of National Counter Proliferation Center*

Section 1022 of the Intelligence Reform Act added a new Section 119A of the National Security Act of 1947 which provides that the President shall establish a National Counter Proliferation Center (NCPC). Under the Act, the Center has seven missions and objectives and should serve as the primary organization within the United States government for analyzing and integrating all intelligence pertaining to proliferation. Among its other powers, the NCPC is authorized to coordinate the counter proliferation plans and activities of all United States government departments and agencies. Section 119A also provided that the NCPC should conduct “strategic operational planning” for the United States government to prevent the spread of weapons of mass destruction, delivery systems, and materials and technologies.

Congress provided the President with the authority to waive any, or all, of the requirements of Section 119A if it was determined that they did not materially improve the nonproliferation ability of the United States. At the time Congress enacted the Intelligence Reform Act, the WMD Commission had not completed its work. Congress provided that the President, after receiving the WMD Commission report, should submit to Congress his views on the establishment of the NCPC.

In its March 31, 2005 report, the WMD Commission recommended that the President establish a relatively small NCPC that manages and coordinates analysis and collection across the Intelligence Community on nuclear, biological, and chemical weapons. The WMD Commission supported the concept of “strategic operational planning,” but recommended that it not be performed by the NCPC.

On June 29, 2005, the White House announced that the President had endorsed the establishment of an NCPC. The statement provided that the NCPC would exercise “strategic oversight” of the Intelligence Community’s weapons of mass destruction activities. The DNI would ensure that the NCPC establishes strategic intelligence collection and analysis requirements regarding WMD that are consistent with United States policies. Under the President’s plan, the NCPC would be established within the Office of the DNI, and the DNI would appoint the Director of the NCPC who would then report to the DNI. On August 8, 2005, the DNI announced the appointment of the first Director of the NCPC. This appointment

represents an important first step in the establishment of the NCPC.

Section 409 of this Act reflects the President's determination that the DNI should appoint the Director of the NCPC and that the NCPC should be located in the Office of the DNI.

Section 409 does not amend any other procedural or substantive provision of Section 119A of the National Security Act of 1947. If the President determines not to assign to the NCPC any power provided by Section 119A, notice must be provided to Congress in writing as required by that section.

*Section 410. Operational files in the Office of the Director of National Intelligence*

Section 410 adds a new Section 700 to the National Security Act of 1947. It ensures that protected operational files provided by elements of the Intelligence Community to the Office of the DNI carry with them any exemption such files had from Freedom of Information Act (FOIA) requirements for search, review, publication, or disclosure.

In the CIA Information Act, Congress authorized the DCI to exempt operational files of the CIA from several requirements of the FOIA, particularly those requiring search and review in response to FOIA requests. In a series of enactments codified in Title VII of the National Security Act of 1947, Congress has extended the exemption to the operational files of the NGA, the National Security Agency (NSA), and the National Reconnaissance Office (NRO). It has also provided that the 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 434 of this Act would extend the FOIA exemption to the operational files of the Defense Intelligence Agency (DIA).

The components of the Office of the DNI, including the National Counterterrorism Center (NCTC), require access to information contained in operational files. The purpose of Section 410 is to make clear that the operational files of any component of the Intelligence Community, for which an operational files exemption is applicable, retain their exemption from FOIA search, review, disclosure, or publication.

The new Section 700 of the National Security Act of 1947 provides several limitations. The exemption does not apply to information disseminated beyond the Office of the DNI. Also, as Congress has provided in the operational files exemptions for the CIA and other Intelligence Community elements, Section 700 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.

In the DNI's request to the Committee for legislative authorities, the Office of the DNI asked for a broader exemption from the FOIA than currently provided in Section 410. The Committee considers it likely that the operations of the Office of the DNI, in particular

the activities of the NCTC and the NCPC, may require an operational files exemption. Before acting on such a request, the DNI, through the Chief Information Officer of the Intelligence Community or other appropriate officers, should systematically study and report to the intelligence committees regarding the application of the FOIA to the Office of the DNI.

As part of this review, the DNI should report on the responsibility assigned by Congress in the Intelligence Reform Act concerning operational file exemptions. Congress amended each operational file statute to provide that the exemption should be made only with the coordination of the DNI. Congress also provided that the decennial review of the exemptions in force must be undertaken with the DNI. These decennial reviews must include consideration of the historical value or other public interest in categories of files and the potential for declassifying a significant amount of the material in them. The DNI should advise the intelligence committees on the benefits of coordinating the four decennial reviews (five with the enactment of Section 434 of this Act) which now occur at different times.

*Section 411. Eligibility for incentive awards of personnel assigned to the Office of the Director of National Intelligence*

Section 411 updates Section 402 of the Intelligence Authorization Act for Fiscal Year 1984 (Pub. L. No. 98-215 (Dec. 9, 1983)) to reflect and incorporate organizational changes made by the Intelligence Reform Act. Section 411 also makes other technical and stylistic amendments and strikes a subsection of the law that applied only during fiscal year 1987.

*Section 412. Repeal of certain authorities relating to the Office of the National Counterintelligence Executive*

Section 412 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 appointed by, and reported to, the President. Those authorities are unnecessary, redundant, and anomalous now that the NCIX is to be appointed by, and under the authority, direction, and control of the DNI.

*Section 413. 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. The FACA sets forth the responsibilities of Congress and the Executive Branch with regard to such committees and outlines procedures and requirements for such committees. As originally enacted in 1972, the FACA expressly exempted advisory committees utilized by the CIA and the Federal Reserve System. Section 413 amends the FACA to extend this exemption to those advisory committees established or used by the Office of the DNI.

*Section 414. Membership of the Director of National Intelligence on the Transportation Security Oversight Board*

Section 414 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 Director of the CIA.

*Section 415. Temporary inapplicability to the Office of the Director of National Intelligence of certain financial reporting requirements*

Section 3515 of Title 31, United States Code, requires certain United States government agencies to prepare and submit to the Congress and the Director of the OMB, not later than March 1 of each year, an audited financial statement for the preceding fiscal year. Section 3515 applies to the Office of the DNI. When the Accountability of Tax Dollars Act of 2002 (Pub. L. No. 107-289 (Nov. 7, 2002)), amended Section 3515, the Director of the OMB was given the authority to waive the audited financial reporting requirements for up to two fiscal years for any newly covered agency. Section 3515 was later amended to allow the Director of the OMB to waive the reporting requirements for a covered agency if the budget authority for the agency did not exceed \$25 million (in the given fiscal year) and if the Director of the OMB determined that there was an absence of risk associated with the agency's operations. The Director of the OMB cannot use this limited waiver authority to grant a grace period for the Office of the DNI. Although the former Community Management Staff (CMS) has taken significant strides to address the financial management issues of the Office of the DNI, the DNI requested a grace period from the audited financial reporting requirements of Section 3515.

Section 415 exempts the Office of the DNI from the requirements of Section 3515 for fiscal years 2005, 2006, and 2007. This grace period will give the DNI the necessary time to establish a financial management system for the Office of the DNI that will be able to generate financial statements that meet the prescribed legal and auditing standards. The Committee expects the DNI to work diligently to bring the Office of the DNI into compliance with the requirements of Section 3515. Notwithstanding the length of the waiver provided in Section 415, the Committee strongly encourages the DNI to ensure compliance with the requirements of Section 3515 at the earliest possible date.

*Section 416. Applicability of the Privacy Act to the Director of National Intelligence and Office of the Director of National Intelligence*

The Privacy Act (5 U.S.C. 552a) has long contained a provision under which the Director of the CIA 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 adequate and appropriate 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 Office of the DNI. Section 416 extends to the DNI the authority to promulgate rules under which certain

records systems of the Office of the DNI may be exempted from certain Privacy Act disclosure requirements.

*Section 417. Temporary exemption from personnel limits of certain Office of Director of National Intelligence personnel assigned to the National Counterterrorism Center*

Section 1096 of the Intelligence Reform Act authorizes within the Office of the DNI only 500 new personnel positions during fiscal years 2005 and 2006. The Committee is concerned that Section 1096 places an artificial limitation on the ability of the DNI to create permanent personnel positions within the NCTC. As currently constructed, the NCTC relies on detailees from other Intelligence Community elements. To ensure institutional memory and build an NCTC analytic base independent of any particular Intelligence Community element, the Committee strongly encourages the development of a permanent cadre of analysts at the NCTC. To promote the creation of this permanent cadre, Section 417 of this Act exempts permanent positions within the NCTC from the application of the personnel limitations in Section 1096. Section 417 will permit the creation of a permanent cadre at the NCTC-administratively a part of the Office of the DNI-without interfering with the DNI's ability to create permanent positions elsewhere within the Office, including a permanent cadre charged with the coordination and management of the Intelligence Community.

Subtitle B—Central Intelligence Agency

*Section 421. Director and Deputy Director of the Central Intelligence Agency*

The Intelligence Reform Act established the positions of the DNI and the Principal Deputy Director of National Intelligence (PDDNI) and abolished the positions of DCI and Deputy Director of Central Intelligence as those positions had previously existed. The DNI and PDDNI are responsible for leading the entire Intelligence Community, which includes many components from the DoD. Moreover, the DNI and PDDNI must ensure that the war fighter continues to receive timely, actionable intelligence. Accordingly, the Intelligence Reform Act continued the tradition of permitting a commissioned officer to serve as either the leader or principal deputy of the Intelligence Community, so long as both positions are not filled by commissioned officers at the same time.

In establishing the positions of DNI and PDDNI, the Act separated the leadership of the Intelligence Community from the leadership of the CIA. Although the Act explicitly provided for a Director of the CIA, it did not provide for a statutory deputy to the Director.

Section 421 establishes the position of Deputy Director of the CIA. The Deputy Director will be appointed by the President, by and with the advice and consent of the Senate, and will assist the Director of the CIA in carrying out the duties and responsibilities of that office. In the event of a vacancy in the position of Director of the CIA, or during the absence or disability of the Director, the Deputy Director will act for, and exercise the powers of, the Director. The DNI will recommend a nominee to the President to fill any vacancy in this position.

With the amendments made by Section 421, the Presidential nomination of both the Director and Deputy Director of the CIA must be confirmed by the advice and consent of the Senate. Given the sensitive operations of the CIA, nominees for the positions of Director and Deputy Director of the CIA merit close scrutiny by Congress to examine the nominees' qualifications prior to their assumption of the duties of these offices. With respect to the Deputy Director of the CIA, the requirement for Senate confirmation also provides assurance that, in the event of a vacancy in the position of Director of the CIA, or during the absence or disability of the Director, Congress will have previously expressed its confidence in the ability of the nominee to assume those additional duties.

Section 421 also requires that both the Director and Deputy Director of the CIA be appointed "from civilian life." The considerations that encourage appointment of a military officer to the position of DNI or PDDNI do not apply to the leadership of the CIA. Indeed, given the CIA's establishment in 1947 as an independent civilian intelligence agency with no direct military or law enforcement responsibilities, the Committee does not believe that a similar construct of military leadership is appropriate at that agency. Accordingly, the Committee recommends that both the Director and Deputy Director of the CIA should be appointed from civilian life. To preserve the important liaison relationship between the military and the CIA, Section 426 of this Act removes a limitation that might have otherwise discouraged the appointment of a military officer to serve as the Associate Director of the CIA for Military Support. In Section 426, the Committee recognizes the important role played by the Associate Director of the CIA for Military Support by ensuring that an officer of the armed forces assigned to the position cannot be counted against the numbers and percentages of the grade of that officer authorized for that officer's armed force.

Unlike the requirement that the Secretary of Defense be appointed "from civilian life" (see 10 U.S.C. 113(a)), Section 421 does not contain any limitation on how long a nominee must have been "from civilian life" prior to appointment. The only restriction is that an active duty officer must first retire or resign his or her commission and return to civilian life prior to being appointed as either the Director or Deputy Director of the CIA. Thus, the President retains the flexibility to nominate candidates with significant military experience for either or both positions.

The Committee recognizes that the person presently engaged in the administrative performance of the duties of the Deputy Director of the CIA is an active duty commissioned officer. The prohibition on an active duty commissioned officer serving as the Deputy Director of the CIA and the requirement that the position be filled by a Presidential nominee confirmed by the Senate will not take effect until the earlier of the date the President nominates an individual to serve in such position or the date the individual presently performing the duties of that office leaves the post. To insulate the current officer from undue military influence, Section 421 provides that so long as the individual continues to perform the duties of the Deputy Director of the CIA, he may continue to receive military pay and allowances, but he is not subject to the supervision or con-

trol of the Secretary of Defense or any of the military or civilian personnel of the DoD, except as otherwise authorized by law.

*Section 422. Enhanced protection of Central Intelligence Agency intelligence sources and methods from unauthorized disclosure*

Section 422 amends the National Security Act of 1947 to provide the Director of the CIA the authority to protect CIA intelligence sources and methods from unauthorized disclosure, consistent with any direction from the President or the DNI. Prior to the Intelligence Reform Act, the authority to protect intelligence sources and methods had been assigned to the DCI, as head of the Intelligence Community. The CIA relied on the DCI's sources and methods authority as the CIA's primary statutory basis for protecting a range of CIA information, including its human sources, from public or unauthorized disclosure in a wide range of contexts and proceedings. This authority proved critical for assuring current and potential human intelligence sources that CIA could, and would, keep the fact of their association with the United States government secret, whether in civil litigation, administrative proceedings, or other arenas. In Section 102A(i) of the National Security Act, as added by the Intelligence Reform Act, Congress transferred this DCI authority to the DNI.

At the request of the Office of the DNI, Section 422 would supplement that grant of authority to the DNI with a comparable grant to the Director of the CIA, subject to the direction of the President or DNI. It is intended to underscore for intelligence sources that the CIA has explicit statutory authority to protect its sources and methods. The revision to Section 104A(d) of the National Security Act of 1947 is not intended to, and does not, authorize the Director of the CIA to withhold from the DNI any CIA information to which the DNI is entitled by statute, Executive Order, Presidential directive, or other applicable law or regulation.

Section 422 also makes conforming changes to Section 6 of the CIA Act of 1949.

*Section 423. Additional exception to foreign language proficiency requirement for certain senior level positions in the Central Intelligence Agency*

Section 423 modifies statutory provisions pertaining to foreign language proficiency for certain senior officials in the CIA. Currently, Section 104A(g) of the National Security Act of 1947 (Section 421 of the Committee's bill results in the re-designation of Section 104A(g) as 104A(h)) provides that an individual cannot be appointed to a position in the Senior Intelligence Service (SIS) in the CIA's Directorate of Intelligence (DI) or Directorate of Operations (DO) unless the individual demonstrates at least a specified level of professional speaking and reading proficiency in a foreign language. Current law also grants the Director of the CIA limited authority to waive this requirement with respect to a position or class of positions with notification to the intelligence committees.

Section 423 enhances CIA management flexibility by authorizing the Director of the CIA to waive the foreign language proficiency requirement, not just with respect to positions or categories of positions, but also as to individual officers or categories of individual officers-subject to the Director of the CIA's determination that such

proficiency is not necessary for the successful performance of the duties and responsibilities involved. The section also adds a “grandfather” clause to the language proficiency requirement, creating a transition period that will allow CIA leadership to more effectively manage the senior Agency workforce during a critical period of change. Finally, Section 423 makes appropriate conforming changes to the report on waivers currently required by Section 104A(g).

The Committee expects the CIA to move forward in its commitment to enhance its overall language capabilities. The personnel flexibility granted by Section 423 will allow the Director of the CIA to better integrate requirements for language skills into leadership training, promotion, and retention decisions and to plan for the projected influx of new DI and DO officers.

*Section 424. Exclusion of the Central Intelligence Agency from annual report on improvement of financial statements for auditing purposes*

Section 424 repeals the requirement that the Director of the CIA submit to the intelligence committees an annual report describing the activities being undertaken to ensure that financial statements of the CIA can be audited in accordance with applicable law and the requirements of the OMB. The report is unnecessary and duplicative now that CIA has submitted, and will continue to submit, audited financial statements in accordance with the Accountability of Tax Dollars Act of 2002 (Pub. L. No. 107–289 (Nov. 7, 2002)).

*Section 425. Additional functions and authorities for protective personnel of the Central Intelligence Agency*

Section 425 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.

*Arrest Authority*

Section 425 authorizes protective detail personnel, when engaged in the performance of protective functions, to make arrests in two circumstances. Under this section, protective detail personnel may make arrests without a warrant for any offense against the United States—whether a felony, misdemeanor, or infraction—that is committed in their presence. They may also make arrests without a warrant if they have reasonable grounds to believe that the person to be arrested has committed or is committing a felony, but not other offenses, under the laws of the United States.

Regulations, approved by the Director of the CIA and the Attorney General, will provide safeguards and procedures to ensure the proper exercise of this authority. The provision specifically does not grant any authority to serve civil process or to investigate crimes.

By granting CIA protective detail personnel limited arrest authority, the provision mirrors statutes applicable to other Federal law enforcement agencies that are authorized to perform protective functions. The authority provided under this section is consistent with those of other Federal elements with protective functions, such as the Secret Service (see 18 U.S.C. 3056(c)(1)(c)), the State Department’s Diplomatic Security Service (see 22 U.S.C. 2709(a)(5)), and the Capitol Police (see 2 U.S.C. 1966(c)). Arrest au-

thority will contribute significantly to the ability of CIA protective detail personnel to fulfill their responsibilities to protect officials against serious threats without being dependent on the response of Federal, State, or local law enforcement officers. The grant of arrest authority under this amendment is supplemental to all other authority that CIA protective detail personnel have by virtue of their statutory responsibility to perform the protective functions set forth in the CIA Act of 1949.

*Protection of Personnel of the Office of the DNI*

Section 425 also authorizes the Director of the CIA, on request of the DNI, to make CIA protective detail personnel available to the DNI and to other personnel within the Office of the DNI. The DNI, in consultation with the Director of the CIA and the Attorney General, should advise the intelligence committees within 180 days of enactment of this Act on whether this arrangement meets the protective needs of the Office of the DNI or whether other statutory authority is needed.

*Section 426. Modification of exclusion of military officer serving as Associate Director of the Central Intelligence Agency for Military Support from officer strength and distribution-in-grade limitations*

Section 426 amends existing law to reflect the appropriate designation of the “Associate Director of Central Intelligence for Military Support” as the “Associate Director of the Central Intelligence Agency for Military Support.” The provision also ensures that the position will be “non-count” for purposes of Chapter 32 of Title 10, United States Code.

Subtitle C—Defense Intelligence Components

*Section 431. Modification of requirements on disclosure of governmental affiliation by Department of Defense intelligence personnel*

Section 431 provides a necessary, but limited, DoD intelligence exemption to a provision of the Privacy Act (5 U.S.C. 552a). Section 552a(e)(3) of Title 5, United States Code, requires each agency that maintains a system of records to inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual, of:

- (A) The authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
- (B) The principal purpose or purposes for which the information is intended to be used;
- (C) The routine uses which may be made of the information . . . ; and
- (D) The effects on [the individual], if any, of not providing all or any part of the requested information.

To improve the ability of intelligence personnel of the DoD to recruit sources, it is sometimes necessary for Defense intelligence personnel, without having to divulge their affiliation with the DoD

or the United States government, to approach potential sources and collect personal information from them to determine their suitability and willingness to become intelligence sources.

The DCI recognized that compliance with the requirements of Section 552a(e)(3) has the potential to threaten operational relationships, compromise the safety of intelligence officers, and jeopardize intelligence sources and methods. Pursuant to Section 552a(j)(1) of the Privacy Act, the DCI exempted all systems of records maintained by CIA from the requirements of Section 552a(e)(3). See 32 C.F.R. 1901.62(b). Section 552a(j)(2) of the Privacy Act grants a similar exemption to law enforcement personnel. Compliance with Section 552a(e)(3) poses similar risks to Defense intelligence personnel and to the lawful and authorized human intelligence missions of the DoD.

Congress has previously recognized the limitations that Section 552a(e)(3) places on Defense intelligence personnel. Section 503 of the Intelligence Authorization Act for Fiscal Year 1995 (Pub. L. No. 103-359 (Oct. 14, 1994)) granted Defense intelligence personnel a very limited exemption from Section 552a(e)(3). The exemption in Section 503 was limited to a single "initial assessment contact outside the United States." Current counterterrorism and other foreign intelligence operations highlight the need for greater latitude to assess potential intelligence sources, both overseas and within the United States. Providing an additional limited exemption to the Privacy Act to give Defense intelligence officers the same protection enjoyed by the CIA when assessing and recruiting sources should serve to protect these officers, shield their operations from security risks, and improve the ability of the DoD to conduct successful human intelligence operations.

Section 431 does not expand the intelligence collection mission of the DoD. Section 431 also maintains current limitations in Executive Order 12333 and DoD Regulation 5240.1-R concerning the collection and retention of information about U.S. persons. In fact, the legislation codifies several restrictions in Executive Order 12333 and DoD Regulation 5240.1-R that provide protections for U.S. persons.

The Committee expects that the majority of Defense intelligence "assessment contacts" with U.S. persons, whether within or outside the United States, should continue to be "open"—i.e., the U.S. person should be aware that they are talking with a representative of the United States government. Under DoD Regulation 5240.1-R, Defense intelligence officials are required to use the "least intrusive means" for collecting intelligence information. In other words, without meeting specified requirements for more intrusive techniques (such as other-than-overt or "clandestine" approaches), Defense intelligence agents must use overt methods to collect publicly available information or information provided with the consent of the person concerned. Within the United States, a clandestine collection effort may be undertaken to collect foreign intelligence about U.S. persons only under the following specified circumstances:

- (a) The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any U.S. person;
- (b) Such foreign intelligence cannot reasonably be obtained by overt means;

(c) The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation; and

(d) The use of other than overt means has been approved in writing by the head of the Department of Defense intelligence component concerned, or his single designee, as being consistent with [DoD Regulation 5240.1-R].

The regulatory conditions under which Defense intelligence personnel may collect information about a U.S. person are quite rigorous and, in large part, have been incorporated in Section 431. If any condition for collection is not met, then the Defense intelligence component may not utilize the authorities provided in Section 431.

Section 431 amends Section 503 of the Intelligence Authorization Act for Fiscal Year 1995 (Pub. L. No. 103-359 (Oct. 14, 1994)) to permit Defense intelligence personnel, under certain limited circumstances, to make assessment contacts with U.S. persons without providing notice of governmental affiliation. In addition to the restrictions in Executive Order 12333 and DoD Regulation 5240.1-R, the authority may only be exercised within the United States upon a determination by the Director of the Defense Intelligence Agency (DIA), or the single designee of the Director, that:

(a) Foreign intelligence, counterintelligence, security, or other operational concerns require that such notice not be given; and

(b) Such assessment contact is undertaken for the purpose of determining whether such U.S. person possesses, or has access to, foreign intelligence information, and whether such U.S. person is credible or suitable as a source, provided that no assessment contact shall be undertaken . . . for the purpose of acquiring information concerning the domestic activities of any U.S. person.

Section 431 also requires that the DoD maintain records associated with each assessment contact under this provision that describe (1) the authority under which the information was collected, (2) any interagency coordination required before the contact, (3) a brief description of such interagency coordination, (4) the basis for the decision not to disclose governmental affiliation, (5) the nature of the information obtained from the U.S. person as a result of the contact, and (6) whether additional assessment contacts, beyond the initial assessment contact, resulted with the person concerned.

The Committee will closely monitor the DoD's use of the authorities provided by Section 503 (as amended by this section) to ensure that the requirements of the provision, Executive Order 12333, and DoD Regulation 5240.1-R are strictly followed and that the privacy and civil liberties of U.S. persons are appropriately protected.

In addition, Section 431 requires the DNI to examine the legal and regulatory requirements and guidelines applicable to assessment contacts to determine whether such requirements or guidelines should be modified to ensure that appropriate protections are afforded United States persons in the course of such contacts. Section 431 also requires the DNI to modify requirements and guidelines applicable to assessment contacts if the DNI finds such modification appropriate. Nothing in the section, or the amendments made by the section, is to be construed as authority for the collection, retention, or dissemination of information concerning U.S.

persons not otherwise authorized by law, Executive Order, or this section.

*Section 432. Enhancements of National Security Agency training program*

Section 16 of the NSA Act of 1959 (50 U.S.C. 402 note) authorizes the NSA to establish and maintain an undergraduate training program to facilitate the recruitment of individuals with skills critical to the NSA's mission. Under the program, the government has always had the right to recoup the educational costs expended for the benefit of employees whose employment with NSA is "terminated"—either voluntarily by the employee or by the NSA for misconduct.

Section 432 amends Section 16(d) of the NSA Act of 1959 to clarify that "termination of employment" includes situations where employees fail to maintain satisfactory academic performance as defined by the Director of NSA. Such employees shall be in breach of their contractual agreement and, in lieu of any service obligation arising under such agreement, shall be liable for repayment. Failure to maintain satisfactory academic performance has always been grounds for default resulting in the right of the government to recoup the educational costs expended for the benefit of the defaulting employee. Thus, this provision is a clarification of that obligation.

In addition, Section 432 permits the Director of NSA to protect intelligence sources and methods by deleting a requirement that the NSA publicly identify to educational institutions which students are NSA employees. 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 covert 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. Despite the deletion of the disclosure requirement, the Committee expects the 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. 99-690, Part I (July 17, 1986) ("NSA employees attending an institution under the program will have no intelligence function whatever to perform at the institution.").

*Section 433. Codification of authorities of National Security Agency protective personnel*

Section 433 amends the NSA Act of 1959 (50 U.S.C. 402 note) by adding a new Section 20, to clarify and enhance the authority of protective details for the NSA.

New Section 20(a) would authorize the Director of the NSA to designate NSA personnel to perform protective detail functions for the Director and other personnel of the NSA who are designated from time to time by the Director of the NSA as requiring protection. Section 11 of the NSA Act of 1959 presently provides that the Director of NSA may authorize agency personnel to perform certain

security functions at NSA headquarters, at certain other facilities, and around the perimeter of those facilities. The new authority for protective details would enable the Director of the NSA to provide security when the Director or other designated personnel require security away from those facilities.

New Section 20(b) would provide that NSA personnel, when performing protective detail functions, may exercise the same arrest authority that Section 425 provides for CIA protective detail personnel. The arrest authority for NSA protective detail personnel would be subject to guidelines approved by the Director of the NSA and the Attorney General. The purpose and extent of that arrest authority, and the limitations on it, are described in the section-by-section explanation for Section 425. That analysis applies equally to the arrest authority provided to NSA protective detail personnel by Section 20(b).

While this bill provides separately for authority for CIA and NSA protective details, the DNI should advise the intelligence committees whether overall policies, procedure, and authority should be provided for protective services, when necessary, for other elements or personnel (or their immediate families) of the Intelligence Community.

*Section 434. Protection of operational files of the Defense Intelligence Agency*

Section 434 amends the National Security Act of 1947 by adding a new Section 705 governing the “operational files” of the DIA. Section 434 exempts specified files from the publication, disclosure, search, and review requirements of the FOIA (5 U.S.C. 552). Existing authority in the National Security Act of 1947 provides the CIA, NSA, NRO, and NGA with certain FOIA exemptions for defined categories of “operational files.” Under these “operational files” exemptions, the CIA, NSA, NRO, and NGA are relieved of the administrative burden of searching and reviewing sensitive classes of files only to retrieve information that would not be subject to release under the FOIA. With some minor variations to reflect the role of the DoD and the armed services committees of the Congress, Section 434 extends to DIA operational files the same FOIA “search and review” exemptions applicable to CIA operational files—i.e., to those files documenting certain human intelligence, foreign liaison, and technical operations of DIA.

*Section 435. Inspector General matters*

The Inspector General Act of 1978 (Pub. L. No. 95-452 (Oct. 12, 1978)) established 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 Inspectors General were 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.” See 5 U.S.C. App. 2. These Inspectors General 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 administra-

tion 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 government are conducted as efficiently and effectively as possible.

The Inspectors General 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 Inspectors General—authorized by either the Inspectors General Act of 1978 or Section 17 of the CIA Act of 1949—enjoy a degree of independence from all but the head of their respective departments or agencies. These Inspectors General also have explicit statutory authority to access information from their respective departments or agencies or other United States government departments and agencies and may use subpoenas to access information (e.g., from a department or agency contractor) necessary for them to carry out their authorized functions.

The NRO, DIA, NSA, and NGA have established their own “administrative” Inspectors General. Because they are not identified in Section 8G of the Inspector General Act of 1978, however, these Inspectors General lack the explicit statutory authorization to access information relevant to their audits or investigations, or to compel the production of such information via subpoena. This lack of authority has impeded access to information—in particular, information from contractors—that is necessary for these Inspectors General to perform their important function. These Inspectors General also lack the indicia of independence necessary for the Government Accountability Office to recognize the annual financial statement audits of these Inspectors General as compliant with the Chief Financial Officers Act of 1990 (Pub. L. No. 101–576 (Nov. 15, 1990)). This lack of independence also prevents the DoD Inspector General, 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 that 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 Inspectors General to perform their audits and investigations, Section 435 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. 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 these Inspectors General from their post by the heads of their respective office or agency must be promptly reported to the 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 435 permits the DNI or the Secretary of Defense to prohibit the Inspectors Gen-

eral 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—similar to the authority of the Director of the CIA under Section 17 of the CIA Act of 1949 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—provides the President, through the DNI or the Secretary of Defense, a mechanism to protect extremely sensitive intelligence sources and methods or other vital national security interests. The Committee expects that this authority will be rarely exercised by the DNI or the Secretary of Defense.

*Section 436. 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 positions at these agencies. Presently, the President appoints the Directors of NSA and NGA, and 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 such circumstances, Senate confirmation of the officer’s promotion or assignment to that position is the responsibility of the Committee on Armed Services. The review of the Committee on Armed Services, however, relates to the military promotion or assignment and not specifically to the assumption by the individual of the leadership of these critical Intelligence Community elements.

Section 436 provides, expressly and uniformly, that the heads of each of these entities shall be nominated by the President and that such nominations will be confirmed by the advice and consent of the Senate. The NSA, NGA, and NRO play a critical role in the national intelligence mission of the United States government. The spending of these agencies 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 U.S. Government. Section 436 does not alter the role of the Committee on Armed Services in reviewing and approving the promotion or assignment of military officers.

Section 436(b) provides that the amendments made by Section 436 apply prospectively. Therefore, the present Directors of NSA, NGA, and NRO are not affected by the amendments, which will apply initially to the appointment and confirmation of their successors.

*Section 437. Security clearances in the National Geospatial-Intelligence Agency*

Although the NSA and the NGA have much in common as technical collection intelligence agencies administratively linked with the DoD, their present authorities for handling security clearances differ significantly. The Secretary of Defense has delegated to the NSA authority for contracting out background investigations and

performing adjudications on individuals doing work for the agency—both for government employees and contractors. In contrast, the NGA must rely exclusively on the Defense Security Service or the Office of Personnel Management for background investigations and on the DIA for adjudication. The consequences for processing times are dramatic, particularly regarding contractor clearances. According to information provided by the DNI's Special Security Center, the average end-to-end processing times for contractors in July 2005 was 73 days for NSA and 540 days for NGA.

The NGA's long backlog for contractor clearances is deleterious for both the agencies and the contractors that support them. For NGA, the backlog drives up financial costs and makes it more difficult to compete for talent. The backlog also distorts efficiencies and good business practices in the private sector, as contractors adjust to the realities of significantly different agency clearance timelines.

The Committee calls upon the Secretary of Defense and the DNI to remedy this unacceptable situation and to report to the intelligence committees on strategies to mitigate the present situation within 90 days of the issuance of this Report. In so doing, the Committee strongly urges the Secretary of Defense to use all available legal authorities, including the delegation of background investigation and adjudication authorities to the NGA for a time-limited period to reduce current backlogs.

#### Subtitle D—Other Elements

##### *Section 441. Department of Justice intelligence matters*

Section 441 establishes a National Security Division (NSD) within the DoJ, headed by an Assistant Attorney General for National Security (AAGNS). This provision is consistent with the WMD Commission's recommendation that the "Department of Justice's primary national security elements—the Office of Intelligence Policy and Review, and the Counterterrorism and Counterespionage sections—should be placed under a new Assistant Attorney General for National Security." The President endorsed this recommendation in a June 29, 2005, memorandum for the Vice President, Secretary of State, Secretary of Defense, Attorney General, Secretary of Homeland Security, Director of OMB, DNI, Assistant to the President for National Security Affairs, and Assistant to the President for Homeland Security and Counterterrorism.

Like all other Assistant Attorneys General in the DoJ (see 28 U.S.C. 506), the AAGNS will be appointed by the President, with the advice and consent of the Senate. The nomination of any individual by the President to serve as the AAGNS shall be referred to the Committee on the Judiciary and, if and when reported, to the Select Committee on Intelligence for not to exceed 20 calendar days (except that in cases where the 20-day period expires while the Senate is in recess, the Select Committee on Intelligence shall have five additional calendar days after the Senate reconvenes to report the nomination). The Attorney General must obtain the concurrence of the DNI prior to making a nomination recommendation to the President for an individual to serve as the AAGNS.

The AAGNS will be responsible for performing duties assigned by both the Attorney General and the DNI. It is important to note,

however, that the DNI will have no authority through the AAGNS to execute any police, subpoena, law enforcement or prosecution powers or internal security functions not otherwise authorized by law. Section 441 also amends the Foreign Intelligence Surveillance Act of 1978 (FISA) (50 U.S.C. 1801(g)) to allow the AAGNS, upon a designation by the Attorney General, to approve applications for electronic surveillance and physical searches for national security investigations.

The Committee believes that the creation of an NSD within the DoJ is an essential prerequisite for ensuring that the AAGNS can effectively carry out the position's responsibilities. The NSD will be a full element of the Intelligence Community, except those portions or components charged with the investigation or prosecution of domestic terrorism. The NSD budget will be part of the National Intelligence Program, and the Committee strongly urges that the NSD budget should remain unclassified to the fullest extent practicable. Although Section 441 leaves the organization of the NSD to the discretion of the Attorney General, the Committee believes that the NSD's organization and structure should parallel other DoJ divisions. For example, the AAGNS should supervise at least two Deputy Assistant Attorneys General (DAAGs). One of these DAAGs should be a career criminal prosecutor who would supervise the Counterterrorism and Counterespionage sections. The other DAAG would supervise the Intelligence Oversight Section and the FISA Support Section. These sections would perform the responsibilities currently assigned to the Office of Intelligence Policy and Review. The AAGNS should also be afforded a Chief of Staff, an Office of Administration, a Counselor to the Assistant Attorney General, and an Office of Policy and Legislation. Section 441 also permits the Attorney General and the DNI to jointly designate any other element, component, or office of the DoJ (other than the FBI) as a component of the NSD.

Like the Criminal Division, the NSD should be considered a law enforcement agency, albeit one that specializes in the prevention, detection, investigation, neutralization, and prosecution of crimes that threaten the national security. Through its components, the NSD should: (1) advise the Attorney General on all matters relating to the national security activities of the United States; (2) provide oversight of the FBI's intelligence components to ensure that their activities are conducted in accordance with the Constitution and the laws of the United States; (3) supervise the investigation and prosecution of cases affecting national security (e.g., international terrorism, sabotage, espionage, and other national security or foreign intelligence crimes), foreign relations, and the export of military and strategic commodities and technology; (4) supervise and manage the FISA process; (5) formulate legislative initiatives, DoJ policies, and guidelines related to national security; (6) provide legal advice to Federal prosecutors, investigators, and analysts concerning national security legal authorities; (7) conduct training on national security legal topics; (8) conduct liaison activities with other Intelligence Community agencies; (9) facilitate broad access to, and sharing of, foreign intelligence information across the Intelligence Community and with Federal, State, local, and tribal governments; (10) supervise the preparation of the Division's submission for the annual budget; and (11) perform other duties as as-

signed by the Attorney General and DNI. The NSD is expected to actively participate in the Intelligence Community's mission to prevent and otherwise neutralize threats to the national security.

In matters of oversight, the activities of the AAGNS and the NSD will be subject to the shared jurisdiction of the Congressional appropriations, intelligence, and judiciary Committees.

*Section 442. Foreign language incentive for certain non-special agent employees of the Federal Bureau of Investigation*

Section 442 authorizes the Director of the FBI to pay a cash award, up to 5 percent of basic pay, to any FBI employee who uses or maintains foreign language skills in support of FBI analyses, investigations, or operations to protect against international terrorism or clandestine intelligence activities. Such awards are subject to the joint guidance of the Attorney General and the DNI.

The Committee believes that the guidance of the Attorney General and DNI should reward FBI employees who are using one or more foreign languages in the regular performance of their official duties or maintaining proficiency in an obscure language that is of occasional operational significance. An employee should not automatically receive a 5 percent award for proficiency in any language. An FBI employee working in support of the FBI's counterintelligence mission who is fluent in French, German, or Spanish should not be eligible for a foreign language incentive, unless that employee is using those language skills in the regular performance of his or her official duties. However, the joint guidance should recognize that there are certain languages of operational significance that are not used on a routine basis, but for which a significant incentive should be awarded to maintain the necessary proficiency so that the employee can use the skill for operational purposes when the need arises. Finally, the joint guidelines should also provide for enhanced language incentive awards for those employees who use multiple languages in the performance of their duties, provided that no language incentive award can exceed the cap of 5 percent of basic pay.

*Section 443. Authority to secure services by contract for the Bureau of Intelligence and Research of the Department of State*

Section 443 authorizes the Secretary of State, in certain circumstances, to enter into personal services contracts to support the mission of the Department's Bureau of Intelligence and Research (INR). The authority, which is similar to that provided to the DoD (see 10 U.S.C. 129b), will enable INR to obtain the services of personal services contractors to respond to unanticipated surge requirements prompted by emergent events or crises or under unique circumstances (e.g., to provide temporary backup that will permit full-time employees to seek needed training). Personal services contractors, particularly those with previous INR experience, would also be valuable to train and mentor new INR personnel.

*Section 444. Clarification of inclusion of Coast Guard element in the intelligence community*

Section 444 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 444 clarifies that all of the Coast Guard’s intelligence elements are included within the definition of “intelligence community.”

*Section 445. Clarifying amendments relating to Section 105 of the Intelligence Authorization Act for Fiscal Year 2004*

Section 445 clarifies that the establishment of the Office of Intelligence and Analysis within the Department of the Treasury (Section 105 of the Intelligence Authorization Act for Fiscal Year 2004 (Pub. L. No. 108–177 (Dec. 13, 2003))), 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, Pub. L. No. 108–447 (Dec. 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.

TITLE V—OTHER MATTERS

*Section 501. Technical amendments to the National Security Act of 1947*

Section 501 corrects several inadvertent technical anomalies in the National Security Act of 1947 arising from the amendments made to that Act by the Intelligence Reform Act.

*Section 502. Technical clarification of certain references to Joint Military Intelligence Program and Tactical Intelligence and Related Activities*

Section 502 makes technical clarifications to Section 102A of the National Security Act of 1947 to preserve the participation of the DNI in the development of the annual budgets for any successor program or programs of the Joint Military Intelligence Program (JMIP) and Tactical Intelligence and Related Activities. Section 502 also preserves the requirement for consultation by the Secretary of the Defense with the DNI in the reprogramming or transfer of funds involving any successor program or programs of the JMIP.

*Section 503. Technical amendments to the Intelligence Reform and Terrorism Prevention Act of 2004*

Section 503 corrects a number of inadvertent technical errors in the specified sections of the Intelligence Reform Act.

*Section 504. Technical amendment to the Central Intelligence Agency Act of 1949*

Section 504 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 505. Technical amendments relating to the multiyear national intelligence program*

Section 505 updates the “multiyear national foreign intelligence program” provision to incorporate and reflect organizational and nomenclature changes made by the Intelligence Reform Act.

*Section 506. Technical amendments to the Executive Schedule*

Section 506 makes several technical corrections to the Executive Schedule. 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 506 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 507. Technical amendments relating to redesignation of the National Imagery and Mapping Agency as the National Geospatial-Intelligence Agency*

Section 507 makes several technical and conforming changes to existing law to bring these provisions in line with the change in name of the National Imagery and Mapping Agency to the NGA, as provided for in Section 921(b) of the National Defense Authorization Act for Fiscal Year 2004 (Pub. L. No. 108–136 (Nov. 24, 2003)).

COMMITTEE ACTION

*Motion to close*

On September 22, 2005, on the motion of Chairman Roberts, the Committee agreed, by unanimous consent, to close the markup because matters under consideration at the meeting would require the discussion of information necessary to be kept secret in the interests of national defense or the confidential conduct of the foreign relations of the United States.

*Motion to report committee draft bill favorably subject to amendments*

On September 22, 2005, on the motion of Chairman Roberts, by a vote of 15 ayes and 0 noes, the Committee voted to report the bill favorably, subject to amendment. The votes in person or by proxy were as follows: Chairman Roberts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

*Amendments to committee bill*

On September 22, 2005, by a vote of 15 ayes and 0 noes, the Committee agreed to an amendment by Senator Mikulski to require that the Directors of the NSA, NGA, and NRO be appointed by the President, by and with the advice and consent of the Senate. The votes in person or by proxy were as follows: Chairman Rob-

erts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On September 22, 2005, the Committee agreed, by unanimous consent, to an amendment by Senator Mikulski to provide the DNI or the Secretary of Defense with additional authority to delegate security clearance responsibilities to the NGA until December 31, 2007.

On September 22, 2005, by a vote of 8 ayes and 7 noes, the Committee agreed to an amendment by Senator Levin (for himself and Senator Hagel) that would require certain officials to provide to Congress requested intelligence documents and information within 15 days, unless the President refuses to provide the documents or information based on an assertion of a privilege pursuant to the Constitution. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—aye; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On September 22, 2005, by a vote of 9 noes and 6 ayes, the Committee rejected an amendment by Senator Levin to modify Section 307 to require the Director of the FBI to request, on behalf of a lawful and authorized activity of an element of the Intelligence Community, information regarding international terrorism or proliferation of weapons of mass destruction from a non-Intelligence Community element; to require non-Intelligence Community elements to provide terrorism information or information concerning the proliferation of weapons of mass destruction to the Intelligence Community through the FBI; and to modify the date on which certain reports must be filed regarding the pilot program established under Section 307. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—no; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—no; Senator Corzine—aye.

#### COMMITTEE COMMENTS

##### *Appointment of the General Counsel of the Central Intelligence Agency*

Section 20 of the CIA Act of 1949 provides that the General Counsel of the CIA be appointed by the President, with the advice and consent of the Senate. Section 20 of the CIA Act was enacted in 1996 as part of the Intelligence Renewal and Reform Act of 1996 (Section 813, Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293 (Oct. 11, 1996)). Prior to the enactment of Section 20, the Committee had encouraged the creation of the position, consistent with the recommendations of the Church Committee and

the Iran-Contra Committees. At the time Section 20 was enacted, the Committee believed that the nature of the legal advice provided by the CIA General Counsel on sensitive matters such as covert action and other activities merited close scrutiny of the individual performing these duties through appointment by the President and approval of the Senate.

With passage of the Intelligence Reform Act, establishment of the position of DNI, and the creation of a General Counsel of the Office of the DNI, the responsibilities of the CIA General Counsel should be considered in light of the responsibilities of the DNI and the DNI General Counsel. Indeed, the Committee expects that many of the sensitive legal functions previously performed by the CIA General Counsel—on behalf of the former DCI, as both head of the CIA and of the entire Intelligence Community—will now be performed, or closely managed and directed, by the DNI General Counsel. In particular, given the DNI's responsibility under Section 102A(f)(4) of the National Security Act of 1947 to “ensure compliance with the Constitution and laws of the United States by the CIA [and other elements of the Intelligence Community],” the Committee expects that the DNI General Counsel will provide important legal guidance and serve as the primary legal advisor on activities such as covert actions and the collection, analysis, and dissemination of foreign intelligence or counterintelligence information concerning U.S. persons. The Committee's expectations regarding the DNI General Counsel do not diminish the importance of the CIA General Counsel in providing important legal guidance on the sensitive activities of the CIA. The fulfillment of the Committee's expectations may, however, lessen the need to have a CIA General Counsel that is a Presidential nominee, confirmed with the advice and consent of the Senate.

In the request for legislative authorities for fiscal year 2006, the DNI included a provision that would have eliminated the requirement for the CIA General Counsel to be appointed by the President, with the advice and consent of the Senate. Instead, the provision would have granted the appointment authority to the Director of the CIA. Although the Committee has not included this provision in this legislation, it may be appropriate at a later date to revisit the method in which the CIA General Counsel is appointed. In making this determination, the Committee will consider the role the DNI General Counsel fills in providing legal advice on sensitive matters such as covert action and other sensitive activities—roles the Committee envisioned for the CIA General Counsel in 1996. As the Committee monitors the development of the respective roles of the DNI and CIA general counsels, the Committee strongly encourages the President to appoint a qualified candidate to serve as the CIA General Counsel consistent with the advice-and-consent requirements of current law.

*Management of United States Government Human Intelligence Activities*

The collection of timely and useful human intelligence (HUMINT) is crucial to protecting against some of the most serious threats to our national security. Prior to the enactment of the Intelligence Reform Act, the DCI, in his capacity as head of the CIA, had the statutory responsibility for overall direction and coordina-

tion of the nation's human intelligence operations—a responsibility often referred to as the “National HUMINT Manager.” When the position of DNI was established, and leadership of the Intelligence Community and the CIA was separated, the Director of the CIA was given the statutory responsibility for overall direction of the nation's overseas HUMINT operations. Given the Intelligence Community-wide responsibilities and authorities of the DNI, however, the Director of the CIA's authority is now subject to broad authorities granted to the DNI, including the DNI's responsibility to “manage and direct the tasking of, collection, analysis, production, and dissemination of national intelligence by elements of the intelligence community.” See Section 102A(f)(1)(A)(ii) of the National Security Act of 1947 (50 U.S.C. 403–1(f)(1)(A)(ii)).

A number of inquiries have revealed shortcomings and failures of the nation's HUMINT operations. This Committee, the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, the National Commission on Terrorist Attacks upon the United States, and the WMD Commission have all documented instances in which the nation's HUMINT operations were hindered by lack of innovation, aversion to risk, and failure to coordinate. This Committee has also observed that the CIA's DO (acting as the designee of the DCI) did not effectively exercise the authorities of the National HUMINT Manager, often focusing instead on its own structure and operations instead of coordinating a strong, Intelligence Community-wide HUMINT effort. In this regard, the Intelligence Community's HUMINT operations have lacked strong leadership and an effective mechanism to resolve conflicts among Intelligence Community elements attempting to conduct HUMINT operations.

In the wake of the intelligence failures associated with the attacks of September 11, 2001, and the Intelligence Community's assessment of Iraq's weapons of mass destruction program, Congress enacted the Intelligence Reform Act, creating a DNI with the authority, *inter alia*, to establish the objectives, priorities, and guidance for, and direct the collection of, national intelligence. The Committee urges the DNI to use the authorities granted under the Act to directly manage and oversee the conduct of HUMINT operations across the Intelligence Community. Indeed, as elements of the Intelligence Community, such as the DIA and the FBI, and other United States government agencies, such as the DoD, place a greater emphasis on HUMINT operations, it is imperative that the DNI exercise the authority to prioritize, direct, and coordinate the Intelligence Community's HUMINT operations. The Committee expects the DNI, as “National HUMINT Manager,” to provide a level playing field across the community for all elements engaged in HUMINT operations. In furtherance of this goal, the Committee urges the establishment of standards and guidelines for training, coordination, and deconfliction of HUMINT operations and for the allocation of manpower and resources for HUMINT operations across the Intelligence Community. The Committee looks forward to the DNI's efforts in this regard and will work closely with the DNI, and all elements of the Intelligence Community that conduct HUMINT operations, to ensure the authorities and resources necessary to fulfill this important Intelligence Community mission are provided.

Currently, the DNI's staff that manages HUMINT issues is largely composed of former officers from a single Intelligence Community element. The Committee believes that this staff will perform its duties in an evenhanded manner. Unfortunately, however, perception is often as important as reality. The Committee believes it is critical that the DNI move quickly to ensure that all Intelligence Community HUMINT agencies are more adequately represented on the DNI's HUMINT management staff. This action by the DNI will give all Intelligence Community HUMINT elements confidence that the DNI is working to create a level playing field for HUMINT operations.

#### *Defense HUMINT Management Office*

The Committee supports the creation of the Defense HUMINT Management Office (DHMO) as a means of executing DoD objectives under the DoD HUMINT Enterprise, including the intelligence activities of the military department counterintelligence agencies. The Committee also supports full and extensive oversight and coordination of the Department's HUMINT efforts by the DNI.

Following the September 11, 2001, terrorist attacks, the military services have been authorized to rebuild their HUMINT capabilities. Given the number of DoD entities now authorized to collect intelligence through human sources, the Committee expects the DHMO will provide crucial direction, prioritization, and coordination of DoD's various HUMINT activities. Moreover, the Committee expects the DHMO to facilitate the DNI's efforts to direct and prioritize national intelligence activities across the Intelligence Community, including DoD HUMINT collection.

The Committee recommends that the DHMO be granted the authority to direct and control DoD's collection of intelligence through human sources, consistent with the guidance and direction of the DNI. The Committee also expects the Secretary of Defense to work with the DNI to take all appropriate steps to support the operations of the DHMO and to develop standards and procedures for the coordination, consultation, and deconfliction of DoD and other Intelligence Community HUMINT activities.

#### *Treatment of Intelligence Community Detainees*

During his February 16, 2005, testimony in open session before the Committee, then-Director of Central Intelligence Porter Goss stated that the CIA had received a CIA Inspector General report on the treatment of detainees by members of the Intelligence Community. Director Goss stated that he believed that eight of the ten recommendations made by the CIA Inspector General had been implemented by the CIA.

According to the CIA's Office of Inspector General, only five of the ten corrective recommendations have been implemented. The Committee is concerned with this delay in implementation and urges the Director of the CIA, in consultation and coordination with the DNI, to complete the remaining actions recommended by the CIA Inspector General without further delay.

#### *The National Counterterrorism Center and Information Access*

For many years, the Intelligence Community has sought to achieve greater coordination of intelligence analysis and operations

through the creation of centers. Although some successes have been achieved through the use of centers, the Committee is increasingly concerned that the proliferation of “centers” throughout the Intelligence Community may have become a crutch that prevents the fundamental evolution of the Intelligence Community from a stove-piped system of intelligence collectors to a flexible intelligence information enterprise—where data is readily accessible, via technological means, by any Intelligence Community officer or employee with an appropriate security clearance and a need-to-know regardless of the agency that collected the data. To more closely examine this concern, the Committee Audit and Evaluations Staff is conducting an oversight review of the organization of the Intelligence Community around centers.

The Committee is also concerned that limits on information access—whether based on legal interpretations or ineffective policy—are migrating from parent agencies into the NCTC and possibly other centers. When the NCTC and its predecessor, the Terrorist Threat Integration Center (TTIC), were established, the Committee expected that these centers would become models for information access—true interagency information fusion centers, with representation from all concerned Intelligence Community elements and with policies and procedures that transcended previous limitations on information access and distribution, promoting information access across the Intelligence Community and, as appropriate, with other Federal, State, and local officials.

In several instances since the establishment of the TTIC, the Committee has been disappointed by ineffective information dissemination practices at the TTIC and the NCTC. The Committee is extremely frustrated that four years after the terrorist attacks of September 11, 2001, and after Intelligence Community promises to improve information sharing, the Community appears to have made little progress in this regard. The Committee was particularly perplexed by divergent threat analyses preceding the 2004 Presidential election. During this period, separate Intelligence Community elements reached different conclusions on the level of the terrorist threat to the homeland, and the divergence seemed to be based on one element’s lack of access to another element’s intelligence reporting and to associated background information. Each Intelligence Community element brings a unique and critical perspective to its analytic mission, but without timely, equivalent access to intelligence information these analysts—scattered throughout the Intelligence Community but covering similar analytic topics—cannot effectively conduct their respective missions. The Committee has strongly encouraged thoughtful and in-depth intelligence analysis that may lead to separate analytic conclusions, but the underlying analysis must be based on similar data sets or the divergent conclusions add little value to the policymaking process. Indeed, these sorts of divergent conclusions—based on different data—can actually cause significant confusion among policymakers and lead to delays in the implementation of policies and procedures necessary to protect the United States and its interests.

The Committee’s continuing concern with information access does not mean, of course, that all analysts will have access to all data. Rather, the Committee’s construct of “information access” specifically recognizes that only appropriately cleared analysts

working on a specific topic will have access to all information relevant to that topic. In addition to information technology solutions and the removal of legal and policy impediments, the Committee believes that information access by analysts, with a valid need-to-know, will also require the DNI to effectively manage the overall Intelligence Community analytic mission. Historically, this management has been lacking. The Committee is concerned that the nature of analysis is such, particularly as it relates to international terrorism, that every Intelligence Community element wants its analysts' opinion on every intelligence topic. The Committee believes that this distribution of analytic resources leads to inappropriate duplication of effort. While the Committee supports alternative analysis and "red teaming," given the limitation on Intelligence Community analytic resources, the Committee expects the DNI to carefully examine the analysis mission to address the full spectrum of threats, both immediate and strategic. This effort to administer dispersed analytic resources will benefit efforts to promote real "information access."

The effectiveness of the NCTC as an information fusion center has been hindered by a lack of formal procedures to guide NCTC analysts on how information can be distributed from the NCTC back to the analysts' parent agencies. The NCTC presently operates on a loose, informal system that the former Director of the NCTC described as "the rules of the road." Under these "rules," NCTC analysts assigned from their parent agencies are granted access to databases from other Intelligence Community elements—access they would not have had at their parent agencies. If an NCTC analyst finds intelligence reporting based on this database access which he believes should be distributed to other analysts at his parent agency, the analyst must ask a reports officer from the Intelligence Community element responsible for the report to expand its dissemination. If the reports officer denies the request, the NCTC analyst must then ask his superiors at the NCTC, perhaps even the Director of the NCTC, to assist him in his efforts. The NCTC does not have clear procedures in place to guide this process. The NCTC also fails to keep records documenting how often these requests occur and the outcome of the process with respect to each request. This lack of process and metrics is not acceptable. The Committee directs that the DNI draft formal guidelines to address this issue, monitor all instances of requests for broader access to information under these procedures, and track the outcomes of such requests.

The information access problems experienced at the NCTC are a microcosm of the problems confronting the entire Intelligence Community. Arcane policies and procedures—vestiges of a stove-piped intelligence system—continue to prevent broader data-level access to intelligence information. With respect to the applicable statutes, Executive orders, regulations, policies, and legal interpretations that inhibit all-source intelligence analysis, the Committee has now received the report of the ISWG convened by the Intelligence Community Deputies Committee. Based on the work of the ISWG and this Committee's continuing oversight of the Intelligence Community's information access standards, the Committee has included a pilot program in Section 307 of the bill to provide a limited exception to the Privacy Act to permit certain disclosures within the In-

telligence Community and between the Intelligence Community and other departments and agencies of the United States government. The Committee will continue to conduct independent oversight and to review the work of the ISWG to determine whether additional legislative action is required.

*Report on Advanced Analytic Tools and Information Access Impediments*

Congress, in the Conference Report to accompany H.R. 2417, the Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177 (Dec. 13, 2003), directed a report on the application of the Constitution, laws, regulations, Executive orders, and guidelines of the United States to the use of advanced analytic tools by the Intelligence Community. The Committee believed that this report was part of the work of the ISWG, but the issues were not included in that product. The Committee understands that work on this report continues in the Executive Branch, but is quite concerned that the report is now well overdue. The Committee renews its request for a report on these matters. The report by the Attorney General and DNI (now nearly five months overdue) should be provided to the intelligence committees no later than six months after issuance of this Report.

In addition, the Committee directs the Attorney General, Secretary of Homeland Security, and DNI to provide a report to the Committee on the outcome of the review required by Section 4 of Executive Order 13356 (Aug. 27, 2004). Under Section 4, the Attorney General, Secretary of Homeland Security, and former DCI were directed to report to the President their recommendations “on the establishment of Executive Branch-wide collection and sharing requirements, procedures, and guidelines for terrorism information to be collected within the United States, including, but not limited to, from publicly available sources, including nongovernmental databases.” The report was required to be provided to the President by late November 2004. The Committee has not yet been informed of any recommendations contained in the report (or whether that report was ever, in fact, provided to the President).

*Information Technology and Information Access*

As discussed previously, the NCTC’s struggle with information technology and access solutions also highlights greater Intelligence Community-wide difficulties. The development of an Intelligence Community enterprise architecture and shared technological standards for information technology and applications, enforced by a Community-wide manager, is a necessary first step in ensuring secure information exchange across disparate Intelligence Community networks. To that end, the Committee continues to underscore the significance of the position of CIO of the Intelligence Community. See Section 407 of the bill. The Intelligence Community also lacks a comprehensive, coordinated investment portfolio for the research and development of processing, analysis, and collaboration technologies that would enable broader and more sophisticated access by analysts to information lawfully collected by the Intelligence Community. The Committee is concerned that the Intelligence Community continues to devote significant amounts of funding to collection without a comprehensive, balanced investment

in processing, analysis, and collaboration technology. The development and use of these processing, analysis, and collaboration technologies could help address the vast differences in the amount of information the Intelligence Community collects versus the information it actually analyzes. The Committee expects that the DNI, through the CIO of the Intelligence Community, will take appropriate steps to address this deficiency in future budgets for the Intelligence Community.

#### *Classification and Information Access*

Section 102A(i)(2)(A) of the National Security Act directs the DNI to establish and implement guidelines for the classification of information, under applicable law, Executive orders, or other Presidential directives. The Committee strongly recommends that the DNI examine the guidelines and rules for classification, and, as necessary, propose standards for the modernization and simplification of the classification system. This review, and any associated recommendations, should attempt to maximize information access while maintaining limits on the disclosure of truly sensitive intelligence or national security information.

Classification of data by its very nature limits access to information. Although classification is often necessary to protect sensitive intelligence or national security information, overclassification can have serious consequences on the ability of the Intelligence Community to accurately assess information, and on the ability of policymakers to effectively respond to national security threats. Improper classification of information—the disclosure of which would not harm national security—prevents the public from considering national issues in light of all publicly available facts.

In addition to the DNI's responsibilities noted above, Section 1016(d)(3)(A) of the Intelligence Reform Act directs the President to require the heads of Federal departments and agencies to promote a culture of information sharing by reducing disincentives to information sharing, including overclassification. The Committee notes that while some departments and agencies have begun to reduce these disincentives, barriers to effective information access remain. The Committee encourages the President to address the requirements of Section 1016, particularly in the context of the "Information Sharing Environment."

#### *The Information Sharing Environment*

The Intelligence Reform Act also required the creation of the "Information Sharing Environment" ("Environment") for terrorism information. The Environment, when fully implemented, is to be a combination of policies, procedures, and technologies to facilitate the sharing of terrorism information, as appropriate, among Federal, State, local, and tribal governments, and the private sector, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities. By statute, the Environment is to be implemented government-wide. The Committee expects the Program Manager, under the direction, control, and authority of the DNI, to drive the creation of the Environment across the Federal government. The Committee will closely monitor the development of the Environment and its coordination

with the Intelligence Community's own information technology enterprise architecture.

The Committee looks forward to working with the Program Manager to eliminate unreasonable and unnecessary legal and policy impediments to greater information access. In that regard, the Committee awaits the development and implementation of the guidelines required by Section 1016(d) of the Intelligence Reform Act. The Committee directs that the Program Manager report to the Committee regarding the guidelines developed under that section.

*Reorganization of Intelligence Community Elements*

As the President, DNI, and other officials implement the Intelligence Reform Act, consider the recommendations of the WMD Commission, and take other steps to reorganize the elements of the Intelligence Community, the intelligence committees must be kept fully and currently informed of all planned reorganization activities, including efforts to reorganize within elements of the Intelligence Community or reorganize the structure and role of Intelligence Community elements within the parent departments and agencies of such elements. The Committee is aware of reorganization efforts at the CIA, Department of Homeland Security, Federal Bureau of Investigation, and other Intelligence Community elements. All elements of the Intelligence Community engaged in reorganizations should ensure that the DNI is kept fully and currently informed of the activities and is fully coordinated with on all significant decisions.

Congress should also be consulted on any significant decisions to restructure the organization or roles of Intelligence Community elements. Under Title V of the National Security Act of 1947, the DNI, the heads of all elements of the Intelligence Community, and the heads of all departments and agencies of the United States government are required to keep the intelligence committees fully and currently informed of all intelligence activities. The intelligence committees should not be required to consider reorganization plans after they have been finalized. Instead, consistent with the requirements of Title V, the intelligence committees should be provided with sufficient opportunity to review and respond to such proposals. A failure to consult with the intelligence committees during the early stages of planning will increase the likelihood that it is necessary for the committees to act, through legislation or through the annual budget process, to remedy inefficient or ineffective structures resulting from agency reorganizations.

*Report on the Creation of an Intelligence Community Reserve Account*

Since its creation, the CIA has utilized a "reserve for contingencies" that permitted the DCI (now, the Director of the CIA) to transfer funds, with appropriate notification to Congress, to address significant intelligence needs that arise during a fiscal year and that must be addressed outside the normal budget process. The CIA Reserve has proven crucial in permitting the flexibility required to address operational realities as they arise.

As the Committee continues to examine the budgetary and management authorities of the DNI, it may be appropriate to provide

the DNI with a “reserve for contingencies” for use across the Intelligence Community to address emergency needs or operational exigencies. Any grant of authority would require legislative action outlining specific limitations on use, requirements for notification to the intelligence committees, and strong control by the DNI. Under extremely limited circumstances and with prior notification to Congress, it may also be appropriate to permit the DNI to transfer certain limited categories of funds to this reserve account for use without fiscal year limitation. The flexibility of a reserve and the ability to transfer funds to a reserve for later use would require a strong commitment from the DNI to eliminate waste in budget requests and to fully comply with the requirement to produce independent cost estimates for major systems, as required by Section 506A of the National Security Act of 1947. In addition, the DNI would need to closely examine how the reserve account is used so that excessive balances were not maintained in the account over extended periods of time.

To aid the Committee as it considers possible legislative action on this topic, the Committee directs the DNI to provide a report to the intelligence committees within 90 days of release of this Report concerning the possible creation of a “reserve for contingencies” for the Intelligence Community and whether the reserve would provide needed budgetary and operational flexibility. The DNI should also report to the intelligence committees regarding the management of existing reserve accounts, including steps the Office of the DNI will take to ensure that excessive balances are not maintained in these reserves for extended periods. The DNI should also provide any additional information deemed appropriate related to this topic, including any specific recommendations regarding the creation or construction of a “reserve for contingencies” for the Intelligence Community or other authorities needed to provide needed budgetary flexibility.

#### *Central Intelligence Agency Organization*

The CIA is a dynamic organization. For example, the Directorate of Support was created in 2005, and in the last few years, new centers and offices have been created, functions have been consolidated, and new directors, deputy directors, and associate directors have been appointed. To keep up with these changes and to assist in coordination, the CIA widely distributes throughout the Agency an organization chart that is updated quarterly. To assist the Congress in its oversight responsibilities, the Committee directs the CIA to distribute its organization chart to each of the intelligence committees by November 1, 2005, and thereafter to provide those committees with each updated version of the organization chart.

#### *Public Interest Declassification Board*

Section 1102 of the Intelligence Reform Act extends and expands the mandate of the Public Interest Declassification Board. To date, no funds have been made available for the Board to begin operations in fiscal year 2005, and the Administration did not include any money to fund the Board's operations in its budget request for the National Archives and Records Administration for fiscal year 2006. While this omission is understandable, as the Intelligence Reform Act was not passed until well into the budgeting process,

the Committee is recommending the authorization of funds to allow the Board to begin its important work in fiscal year 2006. The Administration should also include sufficient funding for the Board in future budget requests, starting with the fiscal year 2007 budget request, either under the National Archives and Records Administration or another appropriate account.

#### 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 the legislation. On September 29, 2005, the Committee transmitted this bill to the Congressional Budget Office and requested that it conduct an estimate of the costs incurred in carrying out the provisions of this bill.

#### 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 SENATOR SNOWE

I would like to thank the Chairman and the Committee for including Section 408, the Inspector General of the Intelligence Community, in the underlying bill.

As many may know, before the release of the report of the National Commission on Terrorist Attacks upon the United States, I introduced stand-alone legislation-cosponsored by Senator Mikulski, Senator Roberts, and Senator Feinstein—creating an Inspector General for Intelligence. The “Intelligence Community Accountability Act of 2004” proposed an independent Inspector General for the entire Intelligence Community—all fifteen agencies.

The Inspector General that I had envisioned was undoubtedly created in the same vein as the Inspector General that the Committee contemplated when it drafted Section 408. Section 408 stipulates that the Inspector General (IG) of the Intelligence Community (IC):

1. Has the ability to initiate and conduct independent investigations, audits and inspections relating to the programs and operations of the IC, and the relationships between the elements of the IC within the National Intelligence Program and the other elements of the intelligence community ensuring that the office’s jurisdiction is not confined to the National Intelligence Program;

2. Has the ability to recommend policies and the implementation of those policies, enabling the IG to making sweeping recommendations to the entire IC;

3. Provides a means for keeping the Director of National Intelligence (DNI) fully and currently informed of problems and deficiencies, as well the progress of any recommended corrective actions;

4. Shall be appointed by the President and confirmed by the Senate and report directly to the DNI;

5. May only be removed from office by the President;

6. May only be prohibited from initiating, carrying out, or completing an investigation, inspection, or audit by the DNI, and only if the DNI determines that it is vital to national security;

7. Shall have direct and prompt access to the DNI or any employee or any employee of a contractor of any element of the IC and failure to cooperate shall be grounds for appropriate administrative action, including loss of employment;

8. Shall have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material, and the level of classification shall not provide a sufficient rationale for denying the IG access to those materials;

9. Is authorized to receive and investigate complaints from any person and, once such a complaint has been received, the

IG may not disclose the identity of the individual filing the complaint without that person's consent;

10. Shall have the authority to administer to or take an oath, affirmation, or affidavit from any person and such an oath will have the same force and effect as an officer having a seal;

11. Is authorized subpoena power;

12. Shall expeditiously resolve which IG shall conduct an investigation in the event of a matter of jurisdiction of the another IC agency; however the IG of the IC shall make the final decision on the resolution of such jurisdiction;

13. May conduct a separate investigation, inspection, or audit of any matter if the IG of the IC determines that the initial investigation conducted by an IG other than the IG of the IC was deficient;

14. Shall be provided with a staff large enough to carry out the functions of the IG effectively;

15. Shall create a career cadre to provide appropriate continuity;

16. May request information or assistance from any department, agency, or other element of the United States government and upon request of the IG of the IC shall furnish such information or assistance;

17. Shall ensure that each IG of an element within the IC complies fully with a request for information or assistance from the IG of the IC;

18. May, upon reasonable notice, conduct an investigation, inspection, audit of any element in the IC and may enter into any place occupied by any agency giving the IG access to real-time operations;

19. Shall submit to the DNI a classified and unclassified semiannual report summarizing its activities;

20. Shall immediately notify the congressional intelligence committees if the IG, after exhausting all possible alternatives, is unable to obtain documents in the course of an investigation;

21. Shall include in the National Intelligence Program budget a separate account for the office of IG of the IC;

22. Shall not have any duty, responsibility, or function regarding another element of the IC be construed to modify or effect the duties of any other IG; and,

23. Must notify Congress if an investigation of any Senate-confirmed community official is initiated.

These key components were the tenets of my proposed legislation. I would like to, once again, thank the Chairman and the Committee for its valiant effort and commend the drafters of this bill who clearly understand the necessity of a community inspector general.

OLYMPIA J. SNOWE.

ADDITIONAL VIEWS OF SENATORS ROCKEFELLER, LEVIN,  
FEINSTEIN, WYDEN, BAYH, MIKULSKI, AND CORZINE

The process leading up to Committee action on this bill and report followed the long tradition of bipartisanship on the Senate Select Committee on Intelligence. The various provisions in the public legislation and the budget guidance in the classified annex accompanying the bill were the result of extensive consultation and negotiation in which all members' perspectives were heard. Although some members had serious reservations about specific provisions, all members voted to report the bill to the Senate.

There are two areas, however, not directly related to the bill, that reflect a serious disagreement among Committee members. These issues not only reflect a breakdown of the Committee's bipartisan tradition, but a failure in conducting its basic oversight responsibilities. The first is the Committee's very limited progress toward completing the second phase of its inquiry related to pre-war intelligence on Iraq. The second is the Committee's refusal, despite repeated requests from the minority, to initiate a formal review of the many questions surrounding the detention, interrogation and rendition of individuals held in U.S. custody. These two issues are discussed more fully following specific comments related to the bill.

HUMAN INTELLIGENCE AND THE CENTRAL INTELLIGENCE AGENCY

In the past few years, this Committee, and many other commentators, have pointed out the shortcomings of our nation's human intelligence collection efforts. Our spies had not penetrated al Qaida prior to 9/11 and they had not penetrated Saddam's inner circle prior to the Iraq war. The report includes language that could give the impression this problem existed because the Central Intelligence Agency (CIA) had too much authority. The report language suggests the Directorate of Operations has performed so poorly that human intelligence can be improved only by stripping the agency of its position as the Intelligence Community's primary human intelligence collection organization.

This assessment is off the mark and the solution misguided. We had too little intelligence prior to 9/11 and the war in Iraq in part because our nation reduced its investment in intelligence, particularly human intelligence, for a decade beginning in 1989. The understandable desire to cut spending on national security programs after the Cold War led to the closure of CIA stations and bases and a pull back from the CIA's global presence. Other problems certainly affected the CIA as it struggled to transition from the Cold War, but clearly the reduction in resources was a significant factor.

The CIA began rebuilding its cadre of case officers in 1999 and accelerated that process after September 11, 2001. This rebuilding is a lengthy process and it will be some time before we realize all the benefits. But even without the infusion of new talent, the CIA's

Directorate of Operations is populated with dedicated, brave individuals who serve around the world in dangerous assignments with little or no recognition. They are innovative, resourceful and not afraid to take risks, both professional and personal. As we change organizational structures in an attempt to correct the mistakes of the past, we must keep these individuals in mind and make sure we do not do damage to what works.

Section 403 of the bill is designed to ensure that the Director of National Intelligence has the final authority over decisions regarding dissemination of intelligence information from human sources. Language in the report accompanying the bill alludes to problems that have surfaced in the past when information is not shared to the greatest extent practical.

Indeed, both 9/11 and the Iraq intelligence failures have highlighted the need for better information access. But the information access problems identified after those events were not limited to human intelligence; they were structural problems across the Intelligence Community. These structural problems were among the most compelling arguments for the creation of the Office of the Director of National Intelligence (DNI) last year. And in creating that office, the Congress imbued it with the authority necessary to obtain access to all intelligence information and to manage the dissemination of that information.

Given the broad authority provided to the DNI in the Intelligence Reform and Terrorism Prevention Act of 2004, it is unclear why the additional authority of Section 403 is necessary. It also is unclear why the additional authority is required for information related to human intelligence, but no other intelligence discipline.

The report includes language under the heading of "Committee Comments" sharply critical of the Central Intelligence Agency's performance as the "National HUMINT Manager." The report suggests the DNI is better suited for this job.

The Committee certainly should support the DNI and ensure the authority given the office is exercised to the fullest extent and for the betterment the Intelligence Community. But the clear intent of the Congress in passing the Intelligence Reform Act was to create a DNI that manages the Intelligence Community by making use of the considerable expertise that exists within the various agencies. The Director of the National Security Agency is the Intelligence Community functional manager for signals intelligence; the Director of the National Geospatial-Intelligence Agency is the Intelligence Community functional manager for imagery intelligence; and the Director of the CIA has been the Intelligence Community functional manager for human intelligence. There are other elements of the Intelligence Community involved in each of these collection disciplines, but the heads of these agencies are the individuals with the expertise and scope to properly coordinate and deconflict the activities of all the contributing agencies. Any change to these responsibilities is, at best premature, just one year after passage of the Intelligence Reform Act. The DNI was not established as a new bureaucracy to assume the responsibility for day-to-day intelligence operations.

The report language describes the need to have the DNI resolve conflicts among intelligence organizations conducting human intel-

ligence. The language does not, however, describe what those conflicts might be. The CIA has, in fact, recently reached separate agreements with the Federal Bureau of Investigation (FBI) and the Department of Defense to avoid confusion and ensure smooth coordination of human intelligence operations both here and abroad. These negotiations were initiated by the CIA and the other parties involved prior to the establishment of the DNI's office. The DNI has an important role in ensuring the agreements are carried out and effective, but clearly the CIA can play the role of human intelligence manager.

The report also uses the phrase "provide a level playing field" as part of the rationale for making the DNI the National Human Intelligence Manager. This language suggests that the CIA is but one among equals in an array of human intelligence collection agencies. This suggestion is inaccurate. The CIA was established as and remains our nation's primary source for human intelligence collected overseas. The FBI plays a critical role in domestic collection of foreign intelligence and the Defense Department has a smaller but important role in collecting national intelligence. The Defense Department's primary focus, however, is on tactical human intelligence to support military operations. All human intelligence collectors rely on CIA tradecraft standards for highest operational effectiveness. This is a division of labor that can work well, but the CIA must remain in charge.

The Committee needs to monitor the implementation of the Intelligence Reform Act and ensure the Office of the DNI has the authority and resources needed to do the job. And the Committee must closely review the many changes taking place within the CIA as it rebuilds and refocuses its human intelligence collection efforts on today's threats. But as we undertake these oversight responsibilities we must be careful that our actions and words support and not hinder the reform process.

#### CONGRESSIONAL ACCESS TO INFORMATION

The Committee has included two provisions dealing with different aspects of the problem of obtaining sufficient information for the Committee to accomplish its oversight responsibility.

The first provision, Section 107, is the result of an amendment, offered by Senators Levin and Hagel and adopted by the Committee, to require elements of the Intelligence Community to provide, upon request of the Chairman or Vice Chairman of the Senate Intelligence Committee or the Chairman or Ranking Member of the House Intelligence Committee, timely access to intelligence assessments, reports, estimates, legal opinions, or other intelligence information. The requirement would apply unless the President asserted a Constitutional privilege related to the specific documents. This language is similar to a provision included in the Senate-passed version of the intelligence reform legislation last year. That provision was removed in the conference with the House of Representatives.

The second provision is the result of an amendment offered by Senator Corzine to the classified annex accompanying the bill. This classified provision, which addresses specific compartment programs, expresses the frustration of the Committee with the Admin-

istration practice of requesting limits on the number of Committee staff with access to information critical to the Committee's oversight responsibilities. The Committee historically has respected requests to limit access to extremely sensitive material. In some cases, however, these requested limits are overly restrictive and can interfere with the Committee's ability to fulfill its responsibilities and conduct effective oversight of executive branch intelligence programs.

This problem has become more acute because of Administration requests to limit Committee access to certain critical programs regarding the war on terrorism. These programs are of obvious importance to the Committee and individual members. Protecting national security information is paramount and the Committee has a tradition of working cooperatively with the executive branch in establishing access to exceptionally sensitive material. Limitations cannot, however, be allowed to interfere with effective oversight.

LACK OF PROGRESS ON PHASE TWO OF THE COMMITTEE'S INQUIRY  
INTO ISSUES ASSOCIATED WITH PRE-WAR INTELLIGENCE ON IRAQ

On February 12, 2004, the Committee voted unanimously to authorize an inquiry related to pre-war intelligence on Iraq. At that time, an informal Committee inquiry had been underway for almost eight months and the initial tasks were close to complete. The Committee decided to finish this work, issue a report as soon as possible, and tackle additional issues in a second report. The first phase report was issued in July 2004. The delay in completing phase two of the Committee's Iraq inquiry is inexcusable.

The resolution adopted by the Committee last February "refine[d] the terms of reference of the Committee's ongoing inquiry into prewar intelligence with regard to Iraq" to include: (1) whether public statements and reports and testimony regarding Iraq by U.S. Government officials made between the Gulf War period and the commencement of Operation Iraqi Freedom were substantiated by intelligence information; (2) the post-war findings about Iraq's weapons of mass destruction and weapons programs and links to terrorism and how they compare with pre-war assessments; (3) pre-war intelligence assessments about post-war Iraq; (4) any intelligence activities relating to Iraq conducted by the Policy Counterterrorism Evaluation Group and the Office of the Under Secretary of Defense for Policy; and (5) the use by the Intelligence Community of information provided by the Iraqi National Congress. A thorough review of these matters is an essential adjunct to the issues addressed in the Committee's report, "U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq," released in July 2004.

The Committee's press release announcing the decision to expand the inquiry into pre-war intelligence related to Iraq, stated that: "[t]he resolution adopted unanimously today illustrates the commitment of all members to a thorough review, to learning the necessary lessons from our experience with Iraq, and to ensuring that our armed forces and policymakers benefit from the best and most reliable intelligence that can be collected."

Since the Committee identified these so-called Phase Two issues as a high Committee priority in February of last year, the minority

has repeatedly urged completion of the review and been assured that the Committee will fulfill this commitment. Yet despite these repeated assertions, it is clear that only sporadic work has been done on Phase Two since it was authorized. There has been ample time for the Committee to complete the Phase Two inquiry and prepare a written product for member consideration.

The Committee adopted the terms of reference listed above because these questions are central to understanding the events leading to the ongoing war in Iraq. To complete this work requires only one thing—a decision to live up to the Committee’s commitment.

The Committee’s delinquency in addressing an issue that it unanimously voted to address over a year and a half ago has diminished the Committee’s credibility as an effective overseer of the Intelligence Community.

#### OVERSIGHT OF DETENTION, INTERROGATION AND RENDITION PROGRAMS

The Committee adopted three amendments offered by Vice Chairman Rockefeller to the classified annex accompanying the bill related to detention, interrogation and rendition issues. One of these classified amendments, dealing with recommendations from the CIA Inspector General, is described briefly in unclassified language elsewhere in this report. The other two amendments require the CIA and the President to provide certain information to the Congress. The details of those reporting requirements are classified. While these three amendments will help answer some of the questions related to these issues, they are not a substitute for the kind of effective oversight these issues demand.

The controversy surrounding the collection of intelligence using detention, interrogation, and rendition has been growing since the disclosure of the abuses at the Abu Ghraib prison early last year. Since then we have seen a steady flow of allegations of abuse, not just in Iraq, but Afghanistan and Guantanamo Bay as well. While there have been a number of prosecutions and several reviews, no investigation has looked at the full range of issues associated with how these programs have developed, how they are being conducted, and what the long term plans are. These issues fall squarely within our Committee’s jurisdiction.

Interrogation is a major intelligence tool in the war on terrorism and an essential component of the intelligence related to the insurgency in Iraq. Just as it conducts oversight of human, signals, and imagery intelligence collection, the Committee’s obligation under S. Res. 400 “to provide vigilant legislative oversight over the intelligence activities of the United States” requires it to undertake oversight of intelligence collection through interrogation. It is this Committee’s responsibility, not only to answer questions related to abuse, but just as importantly to examine the effectiveness of the methods used in interrogations and the reliability of the information obtained from those interrogations.

Despite repeated attempts to initiate a detailed review of fundamental legal and operational questions surrounding the detention, interrogation and rendition of individuals held in U.S. custody, the Committee majority has refused to conduct such an investigation.

One result of the Committee's failure to thoroughly review these programs is the continued ambiguity in the underlying legal authority creating an ongoing risk to intelligence personnel engaged in these programs. This ambiguity has created serious concerns about the legal and operational protection of intelligence officers involved in detention and interrogation operations. Rules applicable to detention, interrogation, and rendition are the product of treaties, federal statutes, judicial decisions, the legal opinions of the Department of Justice and agency counsel. Unfortunately, in the realm of Department of Justice and agency opinions, there appears to be a body of secret law. To assess the lawfulness and efficacy of current practices, and bring to the attention of the Executive Branch matters requiring reassessment or correction, the Committee should be carefully examining this body of secret legal opinions and operational directives.

One argument put forward by those opposed to a Committee investigation into detention and interrogation matters was the notion that any inquiry would be perceived as an attack on the brave men and women of the Intelligence Community performing these duties. The opposite is in fact true. A full investigation could aid in clarifying the legal and operational ambiguity that currently hampers the program's effectiveness and possibly endangers intelligence personnel. If the Committee is serious about supporting the intelligence officers in the field, we should be pushing the Executive Branch to resolve this and other shortcomings in the detention and interrogation program without further delay.

JOHN D. ROCKEFELLER IV.  
CARL LEVIN.  
DIANNE FEINSTEIN.  
RON WYDEN.  
EVAN BAYH.  
BARBARA A. MIKULSKI.  
JON S. CORZINE.

## ADDITIONAL VIEWS OF SENATORS LEVIN AND WYDEN

From al Qai'da and terrorism to nuclear proliferation and the spread of long range missile capabilities, the United States faces a diversity of threats unique in our history. Understanding the challenges posed by these threats and responding effectively depends on us having reliable information about the capabilities and intentions of our adversaries. A focused, effective intelligence community is essential in this regard. Strong Congressional oversight is critical to ensuring that our intelligence agencies are up to the job.

In the preface to its report, the 9–11 Commission stated that “Congress needs dramatic change . . . to strengthen oversight and focus accountability.” In the 108th Congress, we took some important steps toward that goal in passing both the Intelligence Reform and Terrorism Prevention Act (IRTPA) and a resolution creating the Homeland Security and Governmental Affairs Committee and clarifying certain committee oversight authorities. However, additional reforms are needed.

Effective oversight also depends on Congress having timely access to intelligence information. That sentiment is reflected in S. Res. 400, the resolution that established the Standing Committee of the Senate on Intelligence in the 94th Congress. Section 11(b) of the resolution states that it is the “sense of the Senate that the head of any department or agency of the United States involved in any intelligence activities should furnish any information or document in the possession, custody, or control of the department or agency, or person paid by such department or agency, whenever requested by the select committee with respect to any matter within such committee’s jurisdiction.” However, despite the clear message of S. Res. 400, too often members of Congress, even those of us who are members of committees of jurisdiction, do not have timely access to the intelligence information necessary to do our jobs.

IRTPA was helpful in clarifying Congress’s right to intelligence information. Prior to its passage, Section 103 of the National Security Act (50 U.S.C. 403–3) stated that the Director of Central Intelligence “shall be responsible for providing national intelligence . . . where appropriate to the Senate and House of Representatives and the committees thereof.” (Emphasis added). IRTPA not only shifted that responsibility to the new Director of National Intelligence, but removed the phrase “where appropriate,” thus clarifying that Congress had the same right to national intelligence as elements of the executive branch (IRTPA Section 102A(a)(1)(D)). Unfortunately, in some cases, that right has yet to become a reality.

This problem is not unique to any particular administration. Indeed, it reflects longstanding tension between the executive and legislative branches over their respective roles in national security affairs. However, when those tensions manifest themselves in the

withholding of relevant intelligence information from the Congress, they can have disastrous consequences.

To offer just one example, forty years ago, Secretary of Defense McNamara invoked classified communications intercepts to support passage of the Gulf of Tonkin Resolution, which was used by President Johnson as the legislative foundation for expanding the war against Vietnam. According to John Prados, an analyst at the National Security Archive, Secretary McNamara used the intercepts as a “trump card during the 1964 hearings to silence doubters.” The intercepts later proved dubious. We won’t speculate as to whether Congress’s consideration of the Gulf of Tonkin resolution would have been different if the Johnson administration had given Congress all the relevant intelligence, but the example illustrates why Congressional access to intelligence information is so critical.

During the Senate Intelligence Committee’s consideration of fiscal year 2006 Intelligence Authorization legislation, the Committee adopted an amendment Senator Levin offered with Senator Hagel that is consistent with the changes made by IRTPA and reflects the sentiment of S. Res. 400. A similar provision was included in the version of IRTPA that passed the Senate 96–2 in the 108th Congress, but that provision was removed in conference committee.

The amendment adopted by the Intelligence Committee requires elements of the intelligence community to provide, upon request from Congressional Committees of jurisdiction or the Chairman or Vice Chairman of the Senate Intelligence Committee or Chairman or Ranking Member of the House Intelligence Committee, timely access to intelligence assessments, reports, estimates, legal opinions, or other intelligence information.

The Senate Intelligence Committee has a longstanding non-partisan tradition. The Committee has a Chairman and Vice Chairman, rather than a Chairman and Ranking Member. And, in the Chairman’s absence, the Vice Chairman, rather than the next most senior majority party member of the Committee, acts in his place. Requiring intelligence community elements to respond to requests from either the Chairman or Vice Chairman of the Senate Intelligence Committee, as does the amendment, is in keeping with that tradition.

The amendment’s requirement that the intelligence community respond to Congressional requests for information is intended to apply only to existing documents and other intelligence information. The amendment does not create new authority for the Congress to task the intelligence community to generate new intelligence assessments, reports, estimates, legal opinions, or other intelligence information.

Under the Levin-Hagel amendment, elements of the intelligence community are required to respond to requests for intelligence information unless the President certifies that the documents or information is not being provided because the President is asserting a privilege pursuant to the Constitution.

The Constitution entrusts Congress with important responsibilities in the area of national security. It is the responsibility of Senators to seek information so that we may make informed decisions. The Levin-Hagel amendment will improve Congress’s ability to carry out that responsibility.

During the Committee's consideration of the fiscal year 2006 Intelligence Authorization bill, Senator Levin also offered an amendment to Section 307 of the bill. Section 307 would add an exception to the Privacy Act, permitting the sharing of Privacy Act records between elements of the intelligence community (IC), their parent agencies and other federal agencies, under certain conditions.

Privacy Act records contain sensitive information about American citizens. Veterans' health records at the Veterans Administration, case files compiled by the Equal Employment Opportunity Commission during the investigation of discrimination complaints, and certain mental health records maintained by the Department of Health and Human Services, are all protected under the Privacy Act. While it's clear that the IC must improve information sharing, changes to the Privacy Act ought to be carefully considered. With that in mind, we were disappointed that the Committee did not hold any hearings on the changes proposed by Section 307 and Committee members were not afforded the perspective of Privacy Act experts within or outside the government on the proposed changes.

As drafted, Section 307 would arguably not permit the CIA to access Privacy Act records from the Department of Housing and Urban Development (HUD), as HUD does not contain an IC element and, to our knowledge, does not have responsibility for protecting the country against the threat of international terrorism or weapons of mass destruction (WMD). By contrast, simply because it shares a parent agency with the Federal Bureau of Investigation (FBI), an IC element, the bill would permit the CIA to access Privacy Act records from the Department of Justice's Civil Rights Division as long as the records related to a lawful and authorized foreign intelligence or counterintelligence activity of the CIA. This is despite the fact that the DOJ Civil Rights Division, like HUD, does not have the responsibility to protect against the threat of international terrorism or WMD.

It seems unwise to permit sensitive records of American citizens held by DOJ's Civil Rights Division to be disseminated under the terms described in the bill. In addition, the bill's inconsistent treatment of Privacy Act records held by DOJ's Civil Rights Division and similarly situated non-IC entities and those held by HUD and other agencies that do not contain an IC element is illogical. The Levin amendment would have corrected that inconsistent treatment and provided stronger Privacy Act protections than those in the bill by treating DOJ's Civil Rights Division like HUD rather than the FBI.

As discussed above, when certain conditions are met, the Committee reported bill authorizes any IC element to seek Privacy Act records directly from certain non-IC elements. The bill also permits non-IC agencies to initiate sharing of Privacy Act records if the head of the non-IC agency determines that the record constitutes either terrorism information as defined in Section 1016(a)(4) of the National Security Intelligence Reform Act of 2004 or information concerning the proliferation of WMD, and the disclosure is to an appropriate IC element.

Under Executive Order 12333, the Federal Bureau of Investigation is the primary agency responsible for the collection of foreign

intelligence in the United States. The Attorney General has established guidelines as to how those responsibilities are carried out. Consistent with the Bureau's existing responsibilities, the Levin amendment would have required the FBI to coordinate requests from IC elements to non-IC agencies for Privacy Act records and would have designated the FBI as the recipient of Privacy Act records shared by non-IC agencies. The Levin amendment was a modest attempt to improve privacy protections for American citizens and we will continue to pursue such improvements.

Section 307 also directs the Privacy and Civil Liberties Oversight Board to review implementation of the provision. While this may be an appropriate activity for the Board, it should be noted that nearly a year after its statutory creation, the Board has yet to be constituted. In fact, while the President has publicly announced which individuals he intends to appoint to the Board, he has not yet submitted their names to the Senate for confirmation. Ideally, the Committee would have had the benefit of the Board's input prior to considering legislation that directly affects privacy rights. But at a minimum, it would make sense that the Board be constituted before passage of legislation which it has been explicitly directed to monitor and report on.

Finally, we have concerns with Section 431 of the bill. That section would permit certain Department of Defense (DoD) intelligence personnel to meet with and conceal their governmental affiliation from, United States citizens within or outside the United States for the purpose of determining the citizens' access to foreign intelligence information and their suitability as a source. Current law permits DoD intelligence personnel to make one such contact overseas. The legislation reported by the Committee would permit an unlimited number of contacts and would allow them to be made either in the United States or overseas. We believe that DoD intelligence personnel should be required to tell United States citizens in the United States who are not suspected of any wrongdoing that they work for the government. We intend to support changes to this authority as the legislation moves forward.

CARL LEVIN.  
RON WYDEN.

## ADDITIONAL VIEWS OF SENATORS WYDEN AND CORZINE

On June 21, 2005, the Office of the Director of National Intelligence (ODNI) formally transmitted to the congressional intelligence committees the Administration's proposed Intelligence Authorization Act for Fiscal Year 2006. The ODNI also provided to the committees a detailed section-by-section explanation of the provisions in the proposed bill.

As in the past, this part of the Intelligence Community's annual request for legislative authorities is unclassified, in contrast to the Administration's annual request for budgetary authority, which is contained in a classified document. The proposed bill consists of suggested amendments or additions to public law. As an unclassified document that contains recommendations on the enactment of new or modified provisions of public law, there is no reason to treat the document as a secret one.

Next year, the Committee should begin a new practice. The Administration's unclassified request for legislative authorities should be treated as a public document. In that way, other committees and the public will have the opportunity to know what legislative proposals have been placed before the Committee and be able to submit comments to it. The Committee should also proceed as openly as is consistent with national security to consider the Administration's proposals as well as proposals for the enactment of legislative authorities that originate within the Committee.

As other committees, the Committee must meet in closed session when the matters to be discussed will include sensitive national security information. But much of the Committee's discussion of legislative matters concerns issues of policy that should be discussed in open session. And the Committee should hold public hearings on legislative proposals that have a public consequence, such as proposals concerning investigative authorities or the application of the Freedom of Information Act or Privacy Act to the Intelligence Community. In addition to the public's legitimate interest in knowing about proposals that have an impact on it, the Committee would benefit from the insights and information of those whose experiences and expertise may inform the Committee's debate.

RON WYDEN.  
JON S. CORZINE.

○