110TH CONGRESS
2d Session

SENATE

REPORT
110–333

INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2009

MAY 8, 2008.—Ordered to be printed

Mr. ROCKEFELLER, from the Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 2996]

The Select Committee on Intelligence, having considered an original bill (S. 2996) to authorize appropriations for fiscal year 2009 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

CLASSIFIED ANNEX TO THE COMMITTEE REPORT

The classified nature of United States intelligence activities precludes disclosure by the Committee of details of its budgetary recommendations. The Committee has prepared a classified annex to this report that contains a classified Schedule of Authorizations. The Schedule of Authorizations is incorporated by reference in the Act and has the legal status of public law. The classified annex is made available to the Committees of Appropriations of the Senate and the House of Representatives and to the President. It is also available for review by any Member of the Senate subject to the provisions of Senate Resolution 400 of the 94th Congress (1976).

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the Intelligence Authorization Act for Fiscal Year 2009 that is being reported by the Committee. Following that analysis and ex-

planation, the report sets forth Committee comments on other matters. The report also includes additional views offered by Members of the Committee.

TITLE I—BUDGET AND PERSONNEL AUTHORIZATIONS

Section 101. Authorization of appropriations

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for fiscal year 2009.

Section 102. Classified schedule of authorizations

Section 102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities and the applicable personnel levels for fiscal year 2009 are contained in a classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103. Personnel level adjustments

Section 103(a) provides that the Director of National Intelligence (DNI), with approval of the Director of the Office of Management and Budget (OMB), may authorize employment of civilian personnel in fiscal year 2009 in excess of the number of authorized personnel levels by an amount not exceeding 5 percent (rather than the 2 percent in prior law) of the total limit applicable to each Intelligence Community (IC) element under Section 102. The DNI may do so only if necessary to the performance of important intelligence functions. Any exercise of this authority must be reported in advance to the congressional intelligence committees.

Although prior intelligence authorization acts have not defined IC personnel limits in terms of full-time equivalent positions, the Committee has determined it would be consistent with general governmental practice to do so. This will enable IC elements to count two half-time employees as holding the equivalent of one full-time position, rather than counting them as two employees against a ceiling.

In the Administration's request for legislative authorities as part of the Intelligence Authorization Act for Fiscal Year 2008, the DNI asked for broad authority to manage the IC within the limits of available funds but without legislatively-fixed civilian end-strength personnel limits. The DNI's submission to the Committee stated that statutory ceilings have led to increased use of contractors and have hindered the IC's civilian joint duty, student employment, and National Intelligence Reserve Corps programs.

During consideration of the fiscal year 2008 request, the congressional intelligence committees learned that practices within different elements of the Intelligence Community on the counting of personnel are inconsistent, and include not counting certain personnel at all against personnel ceilings. The discretionary authority that is granted to the DNI in Section 103(b) will permit the DNI to authorize Intelligence Community elements to continue their existing methods of counting, or not counting, part-time employees

against personnel ceilings, while ensuring that by the beginning of fiscal year 2010 there is a uniform and accurate method of counting all Intelligence Community employees under a system of personnel levels expressed as full-time equivalents. To ensure that the transition is complete by the beginning of fiscal year 2010, paragraph (4) of Section 103(b) provides that the DNI shall express the personnel level for all civilian employees of the Intelligence Community as full-time equivalent positions in the congressional budget justifications for that fiscal year.

Section 103(c) provides additional flexibility when the heads of IC elements determine that work currently performed by contractors should be performed by government employees. It does so by authorizing the DNI, with OMB's approval, to authorize employment of additional full-time equivalent personnel in a number equal to the number of contractor employees currently performing that work. Any exercise of this authority should be reported in advance to the congressional intelligence committees and should be implemented in accordance with a plan that includes adequate support for personnel. This matter is further addressed in Section 305 of the bill.

Section 104. Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the DNI and sets the authorized full-time or full-time equivalent personnel levels for the elements within the ICMA for fiscal year 2009.

Subsection (a) authorizes appropriations of $696,742,000 for fiscal year 2009 for the activities of the ICMA. Subsection (b) authorizes 944 full-time equivalent personnel for elements within the ICMA for fiscal year 2009 and provides that such personnel may be permanent employees of the Office of the Director of National Intelligence (ODNI) or detailed from other elements of the United States Government.

Subsection (c) provides that personnel level flexibility available to the DNI under Section 103 is also available to the DNI in adjusting personnel levels within the ICMA. Subsection (d) authorizes additional appropriations and personnel for the classified Community Management Account as specified in the classified Schedule of Authorizations and permits the funding for advanced research and development to remain available through September 30, 2010.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $279,200,000 for fiscal year 2009 for the Central Intelligence Agency (CIA) Retirement and Disability Fund.

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

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

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Subtitle A—Personnel Matters

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

Section 301 provides that funds authorized to be appropriated by this Act for salary, pay, retirement, and other benefits for federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in compensation or benefits authorized by law.

Section 302. Enhanced flexibility in non-reimbursable details to elements of the intelligence community

Section 302 expands from one year to up to three years the length of time that United States Government personnel may be detailed to the ODNI on a non-reimbursable basis under which the employee continues to be paid by the sending agency. To utilize this authority, the joint agreement of the DNI and the head of the detailing element is required. As explained by the DNI, this authority will provide flexibility for the ODNI to receive support from other elements of the IC for community-wide activities where both the sending agency and the ODNI would benefit from the detail.

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

Section 303 adds three subsections to Section 102A of the National Security Act of 1947 (50 U.S.C. 403–1), all intended to promote the DNI's ability to manage all the elements of the IC as a single cohesive community.

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

Subsection 102A (t) provides enhanced pay authority for critical positions in portions of the IC where that authority does not now exist. It allows the DNI to authorize the head of a department or agency with an IC element to fix a rate of compensation in excess of applicable limits with respect to a position that requires an extremely high level of expertise and is critical to accomplishing an important mission. A rate of pay higher than Executive Level II would require written approval of the DNI. A rate of pay higher than Executive Level I would require written approval of the President in response to a DNI request.

Subsection 102A(u) grants authority to the DNI to authorize IC elements, with concurrence of the concerned department or agency head, and in coordination with the Director of the Office of Personnel Management, to adopt compensation, performance management, and scholarship authority that have been authorized for any other IC element if the DNI determines that the adoption of such authority would improve the management and performance of the intelligence community and notice is provided to the congressional intelligence committees no later than 60 days in advance of adoption of the authority.

Section 304. 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 IC 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 CIA employees, to the Director of the CIA.

Section 304 provides that the DNI may delegate the authority in Section 116 of the National Security Act of 1947 to the head of any IC element. This expansion is consistent with the view of the Committee that the DNI should be able to delegate authority throughout the IC when such delegation serves the overall interests of the IC.

Section 304 also provides that the head of an IC element to which travel authority has been delegated is also empowered to delegate it 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 IC. To facilitate oversight, the DNI shall submit the guidelines to the congressional intelligence committees.

Section 305. Annual personnel level assessments for the intelligence community

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

The assessment consists of four parts. First, the assessment must provide basic personnel and contractor information for the concerned element of the Intelligence Community. It requires that the data be compared against current fiscal year, the upcoming fiscal year, and—for government personnel—historical five-year numbers and funding levels. Second, the assessment must include a written justification for the requested funding levels. This requirement is necessary to ensure that any personnel cost cuts or increases are fully documented and justified. Third, the assessment must contain a statement by the DNI that based upon current and projected funding the concerned element will have the internal infrastructure, training resources, and sufficient funding to support

the administrative and operational activities of the requested personnel and contractor levels. Finally, the assessment must contain a list of all contractors that have been the subject of an investigation by the inspector general of any element of the Intelligence Community during the previous fiscal year or that are or have been the subject of an investigation during the current fiscal year.

The Committee believes that the personnel level assessment tool is necessary for the Executive branch and Congress to fully understand the consequences of modifying the Intelligence Community's personnel levels. This assessment process is essential to the adoption and continuation of the personnel level flexibility authority provided in Section 103. In the aftermath of the terrorist attacks on September 11, 2001, the Administration undertook sharp increases in personnel for the Intelligence Community under the assumption that the intelligence deficiencies leading up to the attacks resulted from personnel shortfalls. Various external reviews have also recommended more personnel. Since the attacks, Intelligence Community personnel end strength has grown by about 20 percent.

The Committee originally supported personnel growth as a way to strengthen intelligence collection, analysis, and dissemination, but now questions its previous position for four reasons: (1) the recent history of large scale personnel growth indicates that personnel increases do not improve performance commensurate with the cost; (2) the Administration is not adequately funding the personnel growth it has planned; (3) hiring additional personnel diverts fiscal resources from both current mission and modernization needs; and (4) personnel costs always increase, while budgets do not. Therefore, when overall budgets do not keep pace with inflation and decline in real terms, personnel costs as a percentage of the budget increase each year and divert funds from operations and modernization.

In February 2005, the Committee initiated an audit to examine the full scope of activities and resources necessary to support the Administration's projections for Intelligence Community personnel growth during fiscal years 2006–2011. As a result of this review and further study of the issue, the Committee has concluded that increasing personnel without a plan for enabling those personnel to work productively does not prevent intelligence failures, or guarantee enhanced performance. The Committee also concluded that the Administration has not adequately funded its personnel growth plan and that resources provided for personnel growth in some cases have been at the expense of other programs.

Another concern of the Committee is the Intelligence Community's increasing reliance upon contractors to meet mission requirements. It has been estimated that the average annual cost of a United States Government civilian employee is $126,500, while the average annual cost of a "fully loaded" (including overhead) core contractor is $250,000. Given this cost disparity, the Committee believes that the Intelligence Community should strive in the long-term to reduce its dependence upon contractors. The Committee believes that the annual personnel assessment tool will assist the DNI and the congressional intelligence committees in arriving at an appropriate balance of contractors and permanent government employees.

Subtitle B—Acquisition Matters

Section 311. Reports on the acquisition of major systems

Section 311 amends Section 102A(q)(C) of the National Security Act of 1947 (50 U.S.C. 403–1(q)(C)) to require additional detail in annual reports currently required from the DNI for each major system acquisition by an element of the Intelligence Community.

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

Section 311 includes definitions for "acquisition cost," "full life-cycle cost," "intelligence program," "major contract," "major system," and "significant test and evaluation."

Section 312. Vulnerability assessments of major system

Section 312 adds a new oversight mechanism to the National Security Act of 1947 (50 U.S.C. 413 et seq.) that requires the DNI to conduct an initial vulnerability assessment and subsequent assessments of every major system and its significant items of supply in the National Intelligence Program (NIP). The intent of the provision is to provide Congress and the DNI with an accurate assessment of the unique vulnerabilities and risks associated with each NIP major system to allow a determination of whether funding for a particular major system should be modified or discontinued. The vulnerability assessment process will also require the various elements of the Intelligence Community responsible for implementing major systems to give due consideration to the risks and vulnerabilities associated with such implementation.

Section 312 requires the DNI to conduct an initial vulnerability assessment on every major system and its significant items of supply proposed for the NIP prior to completion of Milestone B or an equivalent acquisition decision. The minimum requirements of the initial vulnerability assessment are fairly broad and intended to provide the DNI with significant flexibility in crafting an assessment tailored to the proposed major system. Thus, the DNI is required to use at a minimum, an analysis-based approach to identify vulnerabilities, define exploitation potential, examine the system's potential effectiveness, determine overall vulnerability, and make recommendations for risk reduction. The DNI is obviously free to adopt a more rigorous methodology for the conduct of initial vulnerability assessments.

Vulnerability assessment should continue through the life of a major system and its significant items of supply. Numerous factors and considerations can affect the viability of a given major system. For that reason, Section 312 provides the DNI with the flexibility to set a schedule of subsequent vulnerability assessments for each major system when the DNI submits the initial vulnerability assessment to the congressional intelligence committees. The time period between assessments should depend upon the unique cir-

cumstances of a particular major system. For example, a new major system that is implementing some experimental technology might require annual assessments while a more mature major system might not need such frequent reassessment. The DNI is also permitted to adjust a major system's assessment schedule when the DNI determines that a change in circumstances warrants the issuance of a subsequent vulnerability assessment. Section 312 also provides that a congressional intelligence committee may request the DNI to conduct a subsequent vulnerability assessment of a major system.

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

Section 312 requires the DNI to give due consideration to the vulnerability assessments prepared for the major systems within the NIP. It also requires that the vulnerability assessments be provided to the congressional intelligence committees within ten days of their completion. The conferees encourage the DNI to also share the results of these vulnerabilities assessments, as appropriate, with other congressional committees of jurisdiction. Subsequent vulnerability assessments shall be provided to Congress with the DNI's annual report on major system acquisitions required under Section 102A(q) of the National Security Act of 1947.

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

Section 313. Intelligence community business system modernization

One of the greatest challenges facing the IC today is the modernization of its business information systems. Guidance from the Office of Management and Budget has called for all business information systems in government organizations to become integrated into a business enterprise architecture. A business enterprise architecture incorporates an agency's financial, personnel, procurement, acquisition, logistics, and planning systems into one interoperable system. Currently, each IC element is building unique, stovepiped systems that do not leverage the investments of other elements of the IC. Section 313 gives the DNI a structure for creating a coherent business enterprise architecture that will be use-

ful for the intelligence professional, as well as cost-effective for the taxpayer. The Committee expects that the DNI will include Department of Defense representatives in the established forum as appropriate.

Section 313 requires that the DNI create a business enterprise architecture that defines all IC business systems, as well as the functions and activities supported by those business systems, in order to guide with sufficient detail the implementation of interoperable IC business system solutions. Section 313 also requires the submission of a preliminary draft of the transition plan for implementing the business enterprise architecture. The business enterprise architecture and acquisition strategy are to be submitted to the congressional intelligence committees by March 1, 2009 for all financial management and human resources systems and by March 1, 2010, for all remaining Intelligence Community business systems.

Section 313 will provide the congressional oversight committees the assurance that business systems that cost more than a million dollars and that receive more than 50 percent of their funding from the NIP will be efficiently and effectively coordinated. It will also provide a list of all "legacy systems" that will be either terminated or transitioned into the new architecture. Further, this section will require the DNI to report to the Committee no less often than annually, for five years, on the progress being made in successfully implementing the new architecture.

Section 314. Excessive cost growth of major systems

Section 314 amends Title V of the National Security Act of 1947 (50 U.S.C. 413 et seq.) to require that, in addition to the reporting required under Section 102A(q) of the Act, the program manager of a major system acquisition project shall determine on a continuing basis if the acquisition cost of such major system has increased by at least 25 percent as compared to the baseline of such major system. The program manager must inform the DNI of any such determination and the DNI must submit a written notification to the congressional intelligence committees if the DNI makes the same such determination.

Section 314 is intended to mirror the Nunn-McCurdy provision in Title 10 of the United States Code that applies to major defense acquisition programs. The Committee envisions that the determination will be done as needed by the program manager of the major system acquisition and should not wait until the time that the DNI's annual report is filed. In other words, the Committee expects the congressional intelligence committees to be advised on a regular basis by the DNI about the progress and associated costs of major system acquisitions within the Intelligence Community.

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

adequate to manage and control full life-cycle cost of such major system.

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

If the required certification, at either the 25 percent or 50 percent level, is not submitted to the congressional intelligence committees within 60 days of the DNI's determination of cost growth, Section 314 creates a mechanism in which funds cannot be obligated for a period of time. If Congress does not act during that period, then the acquisition may continue.

Section 315. Prohibition on conflicts of interest in intelligence community contracting

Section 315 prohibits, beginning in fiscal year 2010, the awarding of a contract for the provision of advisory and assistance services related to any major system acquisition with an element of the Intelligence Community to an entity whose business activities include the provision of products or services related to the same major system acquisition.

This provision addresses a continuing concern of the Committee about apparent conflicts of interest within the intelligence acquisition community. Despite provisions in the Federal Acquisition Regulation intended to preclude such conflicts, the Committee is concerned that organizational conflicts of interest may adversely affect major acquisitions.

The Executive branch is increasingly relying upon contractors to assist in managing or integrating complex acquisitions. Contractor advisory and assistance service (CAAS) and systems, engineering, and technical assistance (SETA) contracts are often used to perform what would otherwise be inherently governmental functions. There are merits to the government utilizing the technical and program management expertise that exists in the private sector. Close relationships, however, between CAAS/SETA contractors and their parent, affiliate, or subsidiary companies could bias those contractors in providing advice to the government.

Where a program's prime contractor has a contractor affiliate working in the program office setting program requirements, assisting in source selections, and determining award and incentive fees for the same program, there is strong potential for conflicts of interest. An Inspector General report from an element of the Intelligence Community expressed concern about such apparent conflicts that were negatively impacting the interests of that particular element. Indeed, the Committee notes that several major prime contractors have corporate affiliates supporting government program offices in the management of major Intelligence Community acquisitions. The Committee believes this practice is undesir-

able and has adopted Section 315 to eliminate such conflicts of interest.

Section 315 does not take effect until the beginning of fiscal year 2010. This transition period will allow existing CAAS/SETA contractors to make necessary adjustments to their corporate structures to avoid triggering a violation of Section 315.

Section 316. Future budget projections

Section 316 amends Title V of the National Security Act (50 U.S.C. 413 et seq.) to require the DNI, with the concurrence of the Office of Management and Budget (OMB), to provide the congressional intelligence committees with two future budget projections that together span fifteen years and form the basis of affordability assessments required in this section and in Section 408 of the bill. Section 316 thus ensures that the Intelligence Community will make long-term budgetary projections that span the same time frame as the funding needs of programs it initiates in the budget.

Section 316 requires first a Future Year Intelligence Plan for at least four years after the budget year, which includes the year by year funding plan for each expenditure center and for each major system in the NIP. Section 316 also requires lifecycle cost and milestones for major systems. Section 316 also requires a Long-term Budget Projection ten years beyond the Future Year Intelligence Plan, but at a much higher level of budget aggregation. This Long-term Budget Projection is to be conducted under a constrained budget, but under two alternative sets of assumptions about cost growth—one with virtually no cost growth, the other more in line with experience. Section 316 requires that the Long-term Budget Projection includes a description of whether, and to what extent, the projection for each year for each element of the Intelligence Community exceeds the level that would result from applying the most recent Office of Management and Budget inflation estimate to that element. Both budget projections must be submitted to Congress with the President's budget request.

Section 316 ensures that the Executive branch and Congress will be fully aware of the long-term budgetary impact of a major system acquisition prior to its development or production. This is achieved through a requirement that prior to a major system entering Milestone A and Milestone B or an analogous stage of system development, the DNI must report to the congressional intelligence committees whether and to what extent the proposed major system will increase the Future Year Intelligence Plan and the Long-term Budget Projection for that element of the IC. If the proposed major system is estimated to cause an increase to these future budget projections, then the DNI and OMB Director must issue a determination that the anticipated budget increase is necessary for national security.

Subtitle C—Interrogation and Detention Related Matters

Section 321. Limitation on interrogation techniques

Section 321 prohibits the use of any interrogation treatment or technique not authorized by the United States Army Field Manual on Human Intelligence Collector Operations (U.S. Army Field Manual) against any individual in the custody or effective control of any

element of the Intelligence Community or any instrumentality of an element of the Intelligence Community. This limitation on interrogation conducted by Intelligence Community personnel is similar to the limitation on interrogation conducted by Department of Defense personnel in Section 1002(a) of the Detainee Treatment Act of 2005 (42 U.S.C. 2000dd–0(a)).

Section 321(a) was included in the conference report on the Intelligence Authorization Act for Fiscal Year 2008 that was vetoed by the President on March 8, 2008. The Committee has conducted extensive review of the legality, effectiveness, and appropriateness of CIA's detention and interrogation program. The congressional intelligence committees have held numerous hearings on interrogation-related issues, have had many additional member and staff briefings, and have solicited input from a variety of outside experts on both interrogation and the effects of current U.S. interrogation policy. The adoption of Section 321 through the amendment process at the Committee's mark-up reflects the Committee's belief that the CIA should not use interrogation techniques that go beyond those listed in the U.S. Army Field Manual.

As updated in September of 2006, the U.S. Army Field Manual (FM 2–22.3) provides a detailed and unclassified description of the interrogation process, along with a number of interrogation approaches that can be used to elicit information from detainees. The U.S. Army Field Manual leaves interrogators with significant flexibility to determine what approaches will work in particular situations or with particular detainees; it does not mandate that particular interrogation approach strategies be used in any given situation. The Committee has received testimony that the approaches in the U.S. Army Field Manual are effective at eliciting information from detainees and that they can be appropriately tailored to all detainees, including senior terrorist leaders. The procedures in the U.S. Army Field Manual have also been extensively reviewed to ensure compliance with both "American constitutional standards related to concepts of dignity, civilization, humanity, decency, and fundamental fairness," as well as U.S. obligations under international law, including the four Geneva Conventions of 1949. See U.S. Army Field Manual at 5–21.

In addition to describing interrogation approaches, the U.S. Army Field Manual includes a number of specific prohibitions. In particular, it prohibits "acts of violence or intimidation, including physical or mental torture, or exposure to inhumane treatment as a means of or aid to interrogation." It also explicitly prohibits forcing a detainee to be naked, perform sexual acts, or pose in a sexual manner; placing hoods or sacks over the head of a detainee; using duct tape over the eyes of a detainee; applying beatings, electric shock, burns, or other forms of physical pain; waterboarding; using military working dogs; inducing hypothermia or heat injury; conducting mock executions; and depriving the detainee of necessary food, water, or medical care. Requiring the Intelligence Community to comply with the U.S. Army Field Manual thus prohibits the Intelligence Community's use of these actions as interrogation techniques.

The Committee believes that the 19 techniques and approaches in the Manual are effective and appropriate, regardless of whether they are applied in a military or CIA context or whether the inter-

rogated party is believed to have tactical or strategic intelligence value. The Committee intends that Section 321 binds the CIA to the interrogation approaches in the U.S. Army Field Manual, but does not bind the CIA to specific procedures required of the military that do not translate to the CIA context. For example, the U.S. Army Field Manual requires higher level approval for two of its authorized techniques: the "False Flag" approach requires approval at the O–6 level, "Separation" must be approved at the Combatant Commander level. The Committee does not intend for the CIA to seek or obtain approvals outside of the CIA chain of command for the use of such techniques.

The Committee also considered and rejected the argument that restricting the CIA to the techniques listed in the U.S. Army Field Manual would provide detainees with "the playbook." The Committee has received expert witness testimony, as well as testimony from the Directors of the Federal Bureau of Investigation and the Defense Intelligence Agency, that these interrogation techniques are effective despite being publicly available. Furthermore, the Committee believes that the public awareness of the CIA program and extensive speculation on what interrogation techniques may be authorized provides sufficient information, unfortunately, to potential detainees.

The Committee concluded that the existence of a separate, secret CIA program yields significant damage to international perception of the United States. Section 321 therefore creates one consistent interrogation policy across both the U.S. military and the Intelligence Community. Any individual in the custody or under the effective control of an element of the Intelligence Community may therefore be subject only to those interrogation techniques authorized for use by the U.S. military, that is, the interrogation techniques authorized by the U.S. Army Field Manual.

Section 321(b) defines "instrumentality," with respect to an element of the Intelligence Community, to mean a contractor or subcontractor at any tier of the element of the Intelligence Community. This conforms to the definition of "instrumentality" in Section 323 of the bill but is not intended to indicate any substantive difference to the definition of "instrumentality" found in the Intelligence Authorization Act for Fiscal Year 2008.

Section 322. Prohibition on interrogations by contractors

Section 322 prohibits the use by the CIA of contractors in applying interrogation techniques to educe information. This prohibition is intended to apply any CIA interrogation, whether that program includes the use of so-called "Enhanced Interrogation Techniques" or is conducted under a modified program pursuant to Section 321.

The CIA Director, General Michael Hayden, testified in an unclassified February 2008 Committee hearing that contractors are used as part of the CIA interrogation program. The Committee has done additional review into the use of contractors in this activity, to include the level of training and the backgrounds of the contractors employed, the legality of the use of contractors to perform the function, and the degree to which contractors are used to conduct interrogations instead of CIA personnel.

By adoption of this section through the amendment process at the Committee's mark-up, the Committee determined that for rea-

sons of accountability and control, CIA interrogations should be carried out by CIA staff officers, not by contractors.

Section 323. Notification of International Committee on the Red Cross

Section 323 prohibits the use of funds authorized by this bill to detain any individual who is in the custody or under the effective control of an element of the intelligence community (or an instrumentality thereof) if the International Committee of the Red Cross (ICRC) is not provided, consistent with the practices of the Armed Forces of the United States, notification of the detention of such individual and access to such individual.

The ICRC has been visiting detainees in connection with armed conflict since 1915. In 2006, the ICRC visited 478,000 prisoners of war and detainees in more than 70 countries. Consistent with this role, Department of Defense Directive 2310.01E clearly states that the ICRC "shall be allowed to offer its services during an armed conflict, however characterized, to which the United States is a party." The Committee believes that U.S. armed forces have in place effective arrangements to provide the ICRC with notification and access to military detainees.

The Committee understands that the Department of Defense arrangements establish certain key parameters regarding, among other things, the timeliness of the notification and the nature of the access. The Department of Defense arrangements allow for the collection of intelligence from detainees, while also acknowledging the special role established by international law for the ICRC to monitor compliance with the law of war. The Committee believes that such arrangements provide a workable framework for any individuals in the custody of a U.S. intelligence agency.

The United States has long opposed incommunicado detention around the world as incompatible with our notions of liberty and justice. As recently as March 2008, the U.S. Department of State criticized the governments of North Korea, Burma, and Sri Lanka for engaging in "disappearances" in its 2007 Annual Human Rights Report. From time to time, the United States has found itself in need of obtaining access to U.S. personnel in the custody of another government or armed force. On the day after a collision between a U.S. military aircraft and a Chinese military aircraft (which forced the U.S. aircraft to make an emergency landing in Chinese territory), President George W. Bush said: "The first step should be immediate access by our embassy personnel to our crew members. I am troubled by the lack of a timely Chinese response to our request for this access." Allowing ICRC access to individuals in U.S. custody would strengthen our ability to advocate for appropriate treatment of Americans detained overseas and restore our moral authority to press for respect for human rights around the world.

Section 323(b) provides a rule of construction that clarifies that nothing in this section shall be construed to: (1) create or otherwise imply the authority to detain; or (2) limit or otherwise affect any other rights or obligations which may arise under the Geneva Conventions or other laws, or to state all of the situations in which notification to and access for the ICRC is required or allowed.

Section 323(c) defines "instrumentality" for the purposes of this section to mean, with respect to an element of the intelligence com-

munity, a contractor or subcontractor at any tier of the element of the intelligence community.

Section 324. Report on compliance with the Detainee Treatment Act of 2005 and related provisions of the Military Commissions Act of 2006

Section 324 requires the DNI to submit a classified comprehensive report to the congressional intelligence committees on all measures taken by the ODNI and by any IC element with relevant responsibilities on compliance with detention and interrogation provisions of the Detainee Treatment Act of 2005 and the Military Commissions Act of 2006. The report is to be submitted no later than 45 days after the date of enactment of this Act.

The Detainee Treatment Act provides that no individual in the custody or under the physical control of the United States, regardless of nationality or physical location, shall be subject to cruel, inhuman, or degrading treatment. Congress reaffirmed this mandate in Section 6 of the Military Commissions Act, adding an implementation mechanism that requires the President to take action to ensure compliance including through administrative rules and procedures. Section 6 further provides not only that grave breaches of Common Article 3 of the Geneva Conventions are war crimes under Title 18 of the United State Code, but also that the President has authority for the United States to promulgate higher standards and administrative regulations for violations of U.S. treaty obligations. It requires the President to issue those interpretations by Executive Order published in the Federal Register.

The report required by Section 324 shall include a description of any detention or interrogation methods that have been determined to comply with the prohibitions of the Detainee Treatment Act and the Military Commissions Act or have been discontinued pursuant to them.

The Detainee Treatment Act also provides for the protection against civil or criminal liability for United States Government personnel who had engaged in officially authorized interrogations that were determined to be lawful at the time. Section 324 requires the DNI to report on actions taken to implement that provision.

The report shall also include an appendix containing all guidelines on the application of the Detainee Treatment Act and the Military Commissions Act to the detention or interrogation activities, if any, of any IC element. The appendix shall also include all legal justifications of "any office of the Department of Justice." This requirement is drafted so as to accommodate the concern that the provision might otherwise compel the production of internal deliberative legal materials. The provision therefore seeks only the legal justifications of any office of the Department of Justice that rendered an opinion on the matter.

To the extent that the report required by Section 324 addresses an element of the Intelligence Community within the Department of Defense, that portion of the report, and associated material that is necessary to make that portion understandable, shall also be submitted by the DNI to the congressional armed services committees.

Subtitle D—Reporting Requirements

Section 331. Report on use of contractors by elements of the intelligence community

Several provisions of the bill are aimed at reducing the overall use of contractors by the Intelligence Community. The Committee believes these provisions are necessary for financial and accountability purposes. Section 331 addresses the nature of the activities performed by contractors. The section requires a one-time report to the congressional intelligence committees by the DNI describing the activities within the Intelligence Community that the DNI believes should only be conducted by governmental employees but that are being conducted by one or more contractors, an estimate of the number of contractors performing each such activity, and the DNI's plans, if any, to have such activities performed solely by governmental employees.

The Committee recognizes that there are activities that are more appropriately performed by contractors than government employees—installation and maintenance of information technology is a commonly cited example. The Committee also believes, however, that there are tasks that are "inherently governmental," as that term is described in the Office of Management and Budget Circular A–76, that should be done solely by governmental employees. The Committee leaves it to the DNI's discretion to determine what those activities are, but believes that determining analytic judgments, collecting human intelligence, conducting covert action activities, performing interrogations, and managing personnel are among them.

The Committee is hopeful that the reporting requirement in this section will lead to proposals by the DNI to transition contractor work to government positions, utilizing the authorities provided in Section 103(c) of this Act.

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

Section 332 amends the requirements for notifications to Congress under Sections 502 and 503 of the National Security Act of 1947 (50 U.S.C. 413a & 413b) and the requirements for funds to be authorized under Section 504 of that Act (50 U.S.C. 414). First, Section 332 of the bill requires that, in the event that the DNI or the head of an Intelligence Community element does not provide to all members of the congressional intelligence committees the notification required by Section 502 (relating to intelligence activities other than covert actions) or Section 503 (relating to covert actions) of the National Security Act of 1947, all members of the committees will be provided with a notification of this fact and will be provided with a description of the main features of the intelligence activity or covert action.

Section 332 also extends requirements in Section 502 of the National Security Act of 1947 on the form and contents of reports to the congressional intelligence committees on intelligence activities other than covert actions to the requirements for notifications to Congress under Section 503 of that Act (relating to covert actions). In addition, the section requires that any change to a covert action finding under Section 503 of that Act must be reported to the com-

mittees, rather than the existing requirement to report changes only if they are "significant."

Section 333. Federal Bureau of Investigation intelligence transformation

Section 333 requires the Director of National Intelligence, in coordination with the Director of the Federal Bureau of Investigation, to establish performance metrics and specific timetables related to the progress of the FBI in carrying out nine items specified in the bill to make reforms within the Bureau.

In addition, the DNI is required to submit to the congressional intelligence committees a consolidated report on a semi-annual basis over five years on the progress of the FBI in carrying out these items, including an assessment of the metrics, timetables and corrective actions, and a description of the activities being carried out to ensure the FBI is improving its performance.

Section 334. Incorporation of reporting requirements

Section 334 incorporates into the Act each requirement to submit a report to the congressional intelligence committees contained in the classified annex to this Act.

Section 335. Repeal of certain reporting requirements

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

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

In response to a request from the Director of National Intelligence, the Committee examined some of these recurring reporting requirements. Section 335 therefore eliminates certain reports that were particularly burdensome to the Intelligence Community when the information in the reports could be obtained through other means. It also eliminates reports whose usefulness has diminished either because of changing events or because the information contained in those reports is duplicative of information already obtained through other avenues. It modifies the reporting requirements in three cases to change annual reports to biennial reports.

Because the vast majority of recurring reports provide critical information relevant to the many challenges facing the Intelligence Community today, the Committee ultimately eliminated only six statutory reporting requirements, a very small percentage of the many recurring reports currently requested. The Committee believes that elimination of these reports will help the Intelligence

Community to allocate its resources properly towards areas of greatest congressional concern.

Subtitle E—Other Matters

Section 341. Restriction on conduct of intelligence activities

Section 341 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 342. Clarification of definition of intelligence community under the National Security Act of 1947

Section 342 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 elements of departments and agencies of the United States Government whether or not those departments and agencies are listed in Section 3(4).

Section 343. Modification of availability of funds for different intelligence activities

Section 343 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).

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

Section 344. Additional limitation on availability of funds for intelligence and intelligence-related activities

Section 344 adds to the requirements of Section 504 of the National Security Act of 1947, which specify that appropriated funds may be obligated or expended for an intelligence or intelligence-related activity only if the congressional intelligence committees have been "fully and currently informed" of that activity. Section 344 specifies that the committees should be considered to have been 'fully and currently informed' only if all members of the committees are fully informed or if all members have received a notification

providing the main features of the activity or covert action has been provided as required elsewhere in this section.

Section 345. Limitation on reprogramming and transfer of funds

Section 345 modifies the reprogramming requirements set forth in Section 504 of the National Security Act of 1947 (50 U.S.C. 414) to provide in statute that, following a reprogramming notification from the DNI, Attorney General, or Secretary of Defense, appropriated funds may not be expended for a period of up to 90 days after a request for information about the reprogramming is made by one of the congressional intelligence committees. It also allows the President to authorize the reprogramming, regardless of the 90-day review period, to fulfill an urgent operational requirement (excluding cost overruns) when it is necessary for the Intelligence Community to carry out the reprogrammed activity prior to the completion of the review period set by the congressional intelligence committees.

Section 504 of the National Security Act allows the Intelligence Community a certain degree of flexibility in reprogramming authorized and appropriated funds for higher priority activities based on unforeseen requirements without having to seek additional legislation from Congress. Section 345 of the bill alters this delegation of authority to reprogram and transfer funds by formalizing a maximum time period for review by the congressional intelligence committees and instituting a waiver mechanism to ensure that such review does not hamper urgent operational requirements.

Section 346. Availability to public of certain intelligence funding information

Section 601(a) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (50 U.S.C. 415c (August 3, 2007)) requires the DNI to disclose the aggregate amount of funds appropriated by Congress for the NIP for each fiscal year beginning with fiscal year 2007. Section 601(b) provides that the President may waive or postpone such disclosure if certain conditions are met, beginning with fiscal year 2009. Section 346 changes the year for which the waiver is first available to fiscal year 2010.

Section 347. Increase in penalties for disclosure of undercover intelligence officers and agents

Section 347 amends Section 601 of the National Security Act of 1947 (50 U.S.C. 421) to increase the criminal penalties involving the disclosure of the identities of undercover intelligence officers and agents.

Section 347(a) amends Section 601(a) to increase criminal penalties for individuals with authorized access to classified information who intentionally disclose any information identifying a covert agent, if those individuals know that the United States is taking affirmative measures to conceal the covert agent's intelligence relationship to the United States. Currently, the maximum sentence for disclosure by someone who has had "authorized access to classified information that identifies a covert agent" is 10 years. Subsection (a) of Section 347 of this Act increases that maximum sentence to 15 years.

Currently, under Section 601(b) of the National Security Act of 1947, the maximum sentence for disclosure by someone who "as a result of having authorized access to classified information, learns of the identity of a covert agent" is 5 years. Subsection (b) of Section 347 of this Act increases that maximum sentence to 10 years.

Section 348. Authority to designate undercover operations to collect foreign intelligence or counterintelligence

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

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

Section 348 amends the current delegation level for both the FBI and the Department of Justice. It allows the FBI Director to delegate certifying authority to a level not lower than a Deputy Assistant Director in the National Security Branch. It also allows the Attorney General to delegate the certifying authority to a level not lower than a Deputy Assistant Attorney General in the National Security Division. It should be noted that this delegation level for the Department of Justice remains at a higher level than that which is currently required in criminal undercover operations.

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

Section 349. Language and intelligence analyst training program

Section 922 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Pub. L. No. 108–375) authorized the creation of a pilot program to provide scholarships to prospec-

tive language and intelligence analysts. This program was modeled after the military's Reserve Officer Training Corps and administered by the Director of the National Security Agency. The Committee believes that the results of this pilot program thus far have been encouraging.

Section 349 makes the authorization for this program permanent, and transfers authority to administer the program to the Director of National Intelligence. Section 349 also expands the program's scope by authorizing the DNI to award grants to qualified institutions of higher education to develop relevant courses of study, and provides greater legislative clarity regarding the operation of the program.

Section 350. Extension of authority to delete information about receipt and disposition of foreign gifts and decorations

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

With respect to IC activities, public disclosure of gifts or decorations in the Federal Register has the potential to compromise intelligence sources (e.g., confirmation of an intelligence relationship with a foreign government) and could undermine national security. Recognizing this concern, the Director of Central Intelligence (DCI) was granted a limited exemption from reporting certain information about such foreign gifts or decorations where the publication of the information could adversely affect United States intelligence sources. Section 1079 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458 (December 17, 2004) ("Intelligence Reform Act"), extended a similar exemption to the DNI in addition to applying the existing exemption to the CIA Director.

Section 350 provides to the heads of each IC element the same limited exemption from specified public reporting requirements that is currently authorized for the DNI and CIA Director. The national security concerns that prompt those exemptions apply equally to other IC elements. Section 350 mandates that the information not provided to the Secretary of State be provided to the DNI, who is required to keep a record of such information, to ensure continued independent oversight of the receipt by IC personnel of foreign gifts or decorations.

Gifts received in the course of ordinary contact between senior officials of elements of the Intelligence Community and their foreign counterparts should not be excluded under the provisions of Section 350 unless there is a serious concern that such contacts and gifts would adversely affect United States intelligence sources or methods.

Section 351. Extension of National Commission for the Review of Research and Development Programs of the United States Intelligence Community

The National Commission for Review of Research and Development Programs of the United States Intelligence Community was authorized in the Intelligence Authorization Act for Fiscal Year 2003 (Pub. L. No. 107–306), and lapsed on September 1, 2004. Section 501 renews authority for this Commission by extending the reporting deadline to December 31, 2009, and requiring that new members be appointed to the Commission. This section also authorizes funds for the commission from the Intelligence Community Management Account.

Section 352. Clarifying amendments relating to section 105 of the Intelligence Authorization Act for Fiscal Year 2004

Section 352 changes the reference to the Director of Central Intelligence to the Director of National Intelligence in Section 105 of the Intelligence Authorization Act for Fiscal Year 2004 (Pub. L. No. 108–77 (December 13, 2003)) to clarify that the establishment of the Office of Intelligence and Analysis within the Department of the Treasury, and its reorganization within the Office of Terrorism and Financial Intelligence (Section 222 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H, Pub. L. No. 108–447 (December 8, 2004)), do not affect the authorities and responsibilities of the DNI with respect to the Office of Intelligence and Analysis as an element of the Intelligence Community.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

Subtitle A—Office of the Director of National Intelligence

Section 401. Requirements for accountability reviews by the Director of National Intelligence

Section 401 provides that the Director of National Intelligence shall have new authority to conduct accountability reviews of elements within the Intelligence Community and the personnel of those elements. The primary innovation of this provision is the authority to conduct accountability reviews concerning an entire element of the IC in relation to failures or deficiencies.

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

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

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

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

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

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

Section 402. Authorities for intelligence information sharing

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

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

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

use or identify current-year funding, or concerns regarding the augmentation of appropriations.

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

Section 403. Modification of limitation on delegation by the Director of National Intelligence of the protection of intelligence sources and methods

Section 403 amends Section 102A(i)(3) of the National Security Act of 1947 to modify the limitation on delegation by the DNI (which now extends only to the Principal Deputy DNI) of the authority to protect intelligence sources and methods from unauthorized disclosure. It permits the DNI to delegate the authority to the Principal Deputy DNI or the Chief Information Officer of the IC.

Section 404. Authorities of the Director of National Intelligence for interagency funding

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

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

Under Section 404, the DNI is to submit a report to the congressional intelligence committees by February 1st annually from fiscal year 2010 through fiscal year 2013 providing details on how this authority has been exercised during the preceding fiscal year.

Section 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 IC element, which is slated to take effect on October 1, 2008, applies to the co-location of the headquarters

of the Office of the DNI with the headquarters of any other Intelligence Community agency or element.

In his legislative request for this authorization, the DNI has asked, for the first time, that Congress also provide that "The headquarters of the Office of the Director of National Intelligence may be located in the District of Columbia or elsewhere in the Metropolitan Region, as that term is defined in Section 8301 of title 40, United States Code." The purpose of this request is to provide statutory authorization for the location of the ODNI outside of the District of Columbia.

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

The DNI, in his sectional analysis accompanying his request for this authorization, states that whether a statutory exemption (such as the one provided to the CIA) is needed "is unclear." To aid the Congress in determining—in light of the text of 4 U.S.C. 72, and the precedent of the 1955 legislation on the location of the CIA—whether an exemption is required for the location of the ODNI outside the District of Columbia, the Committee requests that the DNI obtain the legal opinion of the Department of Justice's Office of Legal Counsel on that question. If legislation is required, the policy question about the location of the ODNI can then be addressed in a floor amendment to this authorization.

Section 406. Title of Chief Information Officer of the Intelligence Community

Section 406 expressly designates the position of Chief Information Officer in the Office of the Director of National Intelligence as Chief Information Officer of the Intelligence Community. The modification to this title is consistent with the position's overall responsibilities as outlined in Section 103G of the National Security Act of 1947 (50 U.S.C. 403–3g).

Section 407. Inspector General of the Intelligence Community

Section 1078 of the Intelligence Reform Act authorizes the DNI to establish an Office of Inspector General if the DNI determines that an Inspector General (IG) would be beneficial to improving the operations and effectiveness of the 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 appointed an Inspector General and has granted certain authorities pursuant to DNI Instruction No. 2005–10 (September 7, 2005).

As this Committee urged in reports on proposed authorization acts for fiscal years 2006 through 2008, a strong IG is vital to achieving the goal, set forth in the Intelligence Reform Act, of improving the operations and effectiveness of the Intelligence Community. It is also vital to achieving the broader goal of identifying

problems and deficiencies, wherever they may be found in the IC, with respect to matters within the responsibility and authority of the DNI, including the manner in which elements of the IC interact with each other in providing access to information and undertaking joint or cooperative activities. By way of a new Section 103H of the National Security Act of 1947, Section 407 of this Act establishes an Inspector General of the Intelligence Community in order to provide to the DNI and through reports to the Congress, the benefits of an IG with full statutory authorities and the requisite independence.

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

Under the new subsection 103H(e), the DNI may prohibit the IG from conducting an investigation, inspection, 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 to the intelligence committees within seven days. The IG may submit comments in response to the congressional intelligence committees.

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

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

The IG must submit semiannual reports to the DNI that include a description of significant problems relating to IC programs and operations and to the relationships between IC elements. The reports must include a description of IG recommendations and a statement whether corrective action has been completed. Within 30 days of receiving each semiannual report from the IG, the DNI must submit it to Congress.

The IG must immediately report to the DNI particularly serious or flagrant violations. Within seven days, the DNI must transmit those reports to the intelligence committees together with any comments. In the event the IG is unable to resolve any differences with the DNI affecting the duties or responsibilities of the IG or the IG conducts on investigation, inspection, or audit that focuses on cer-

tain high-ranking officials, the IG is authorized to report directly to the intelligence committees.

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

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

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

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 408. Chief Financial Officer of the Intelligence Community

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

By way of a new Section 103I of the National Security Act of 1947, under Section 408, the IC CFO will, to the extent applicable, have the duties, responsibilities, and authorities specified in the Chief Financial Officers Act of 1990. The IC CFO will serve as the principal advisor to the DNI and the Principal Deputy DNI on the management and allocation of IC budgetary resources, and shall

establish and oversee a comprehensive and integrated strategic process for resource management within the IC. Section 408 charges the IC CFO with ensuring that the strategic plan and architectures of the DNI are based on budgetary constraints as specified in the future budget projections required in Section 316.

Section 408 also charges the IC CFO with ensuring that major system acquisitions satisfy validated national requirements for meeting the DNI's strategic plans and that such requirements are prioritized based on budgetary constraints as specified in the future budget projections required in Section 316. To guarantee this is achieved in practice, under Section 408, prior to obligation or expenditure of funds for major system acquisitions to proceed to Milestone A (development) or Milestone B (production), requirements must validated and prioritized based on budgetary constraints as specified in Section 316.

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

Section 409. Leadership and location of certain offices and officials

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

Section 410. National Space Intelligence Office

The United States maintains a large investment in satellites and this investment has grown dramatically in recent years. These satellites serve the commercial and national security needs of the nation. As such, a loss of any or all of these assets would do tremendous harm to our economy and security.

At the same time, our investment in intelligence collection concerning threats to our interests in space has declined markedly in relation to our overall investment in space systems. Despite this significant overall investment, some estimates indicate that we commit only 10 percent of what we did nearly 25 years ago to the analysis of threats to space systems. Recent international events have only served to highlight this problem.

In an effort to better understand future threats to our space assets, as well as potential threats to the United States from space, Section 410 establishes a National Space Intelligence Office (NSIO). It is not the intent of the Committee that the NSIO be a physical consolidation of existing intelligence entities with responsibilities for various types of intelligence related to space. Rather, the functions of the NSIO, among others delineated in Section 410, will be to coordinate and provide policy direction for the management of space-related intelligence assets as well as to prioritize col-

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

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

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

In the CIA Information Act (Pub. L. No. 98–477 (October 15, 1984) (50 U.S.C. 431 et seq.)), Congress authorized the DCI to exempt operational files of the CIA from several requirements of the Freedom of Information Act (FOIA), particularly those requiring search and review in response to FOIA requests. In a series of amendments to Title VII of the National Security Act of 1947, Congress has extended the exemption to the operational files of the National Geo-Spatial Intelligence Agency (NGA), the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the Defense Intelligence Agency (DIA). It has also provided that files of the Office of the National Counterintelligence Executive (NCIX) should be treated as operational files of the CIA (to the extent they meet the criteria for CIA operational files).

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

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

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

ordinating the five decennial reviews presently required by Title VII.

Section 412. Membership of the Director of National Intelligence on the Transportation Security Oversight Board

Section 412 substitutes the DNI, or the DNI's designee, as a member of the Transportation Security Oversight Board established under Section 115(b)(1) of Title 49, United States Code, in place of the CIA Director or CIA Director's designee.

Section 413. Director of National Intelligence report on retirement benefits for former employees of Air America

Section 413 provides for a report by the DNI on the advisability of providing federal retirement benefits to United States citizens who were employees of Air America or an associated company prior to 1977, during the time that the company was owned or controlled by the United States and operated by the CIA.

There were bills in the Senate and House (S. 651 and H.R. 1276 during the 109th Congress and H.R. 1271 in the 110th Congress) that would have provided federal retirement benefits for those employees. By including Section 413 in this authorization bill, the Committee takes no position on the merits of that legislation.

Although the section invites the DNI to submit any recommendations on the ultimate question of providing benefits, the main purpose of the report is to provide Congress with the facts upon which Congress can make that determination. Accordingly, Section 413 outlines the factual elements required by the report. To aid in the preparation of the report, the section authorizes the assistance of the Comptroller General. Among the elements of the report should be: the relationship of Air America to the CIA, the missions it performed, and the casualties its employees suffered, as well as the retirement benefits that had been contracted for or promised to Air America employees and the retirement benefits Air America employees received.

On September 25, 2007, the CIA provided a three page letter to the congressional intelligence and appropriations committees in response to the Senate Select Committee on Intelligence Report 109–259 to S. 3237, requesting a report on "the advisability of providing federal retirement benefits to United States citizens who were employees of Air America or an associated company prior to 1977, during the time that the company was owned or controlled by the United States and operated by the CIA." Although the letter describes the legal basis for denying federal retirement benefits to employees of Air America, it did not provide the factual background that would allow Congress to make an assessment of whether to provide employees of Air America with federal retirement benefits. The report requested in Section 413 therefore continues to be necessary for a comprehensive exploration of the underlying issues.

Section 414. Repeal of certain authorities relating to the Office of the National Counterintelligence Executive

Section 414 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 un-

necessary now that the NCIX is to be appointed by and is under the authority of the DNI.

Section 415. 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 DCI and then (after enactment of the Intelligence Reform Act) the CIA Director could promulgate rules to exempt any system of records within the CIA from certain disclosure requirements under the Act. The provision was designed to ensure that the CIA could provide safeguards for certain sensitive information in its records systems. In assuming the leadership of the Intelligence Community, the DNI similarly requires the ability to safeguard sensitive information in records systems within the ODNI. Section 414 extends to the DNI the authority to promulgate rules under which records systems of the ODNI may be exempted from certain Privacy Act disclosure requirements.

Section 416. Inapplicability of Federal Advisory Committee Act to advisory committees of the Office of the Director of National Intelligence

Congress enacted the Federal Advisory Committee Act (FACA) (5 U.S.C. App.) to regulate the use of advisory committees throughout the Federal Government. FACA sets forth the responsibilities of the Executive branch with regard to such committees and outlines procedures and requirements for them. As originally enacted in 1972, FACA expressly exempted advisory committees utilized by the CIA and the Federal Reserve System. Section 416 amends FACA to extend this exemption to advisory committees established or used by the ODNI. The DNI should inform the intelligence committees periodically about the composition and use by the ODNI of advisory committees.

Subtitle B—Central Intelligence Agency

Section 421. Inapplicability to the Director of the Central Intelligence Agency of requirement for annual report on progress in auditable financial statements

Section 421 relieves the CIA Director from the requirement in Section 114A of the National Security Act of 1947 to submit to the congressional intelligence committees an annual report describing the activities being taken to ensure that financial statements of the CIA can be audited in accordance with applicable law and the requirements of OMB. Although the Committee remains concerned that the CIA has had minimal success in achieving unqualified opinions on its financial statements, the report required by Section 114A, however, is unnecessary as the Committee now receives annual audits of CIA's financial statements from the CIA Inspector General. The requirements of Section 114A continue to apply to the Directors of NSA, DIA, and NGA.

Section 422. Additional functions and authorities for protective personnel of the Central Intelligence Agency

Section 422 amends Section 5(a)(4) of the CIA Act of 1949 (50 U.S.C. 403f(a)(4)) which authorizes protective functions by designated security personnel who serve on CIA protective details.

Section 422 authorizes protective detail personnel, when engaged in, and in furtherance of, the performance of protective functions, to make arrests in two circumstances. 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. The provision specifically does not grant any authority to serve civil process or to investigate crimes.

Section 422 provides that the CIA Director and the Attorney General will issue regulations or guidelines that will provide safeguards and procedures to ensure the proper exercise of this authority. These shall be provided to the congressional intelligence committees.

The authority provided by this section is consistent with those of other Federal elements with protective functions, such as the Secret Service (18 U.S.C. 3056(c)(1)(C)), the State Department Diplomatic Security Service (22 U.S.C. 2709(a)(5)), and the United States Capitol Police (2 U.S.C. 1966(c)). The grant of arrest authority is supplemental to all other authority CIA protective detail personnel have by virtue of their statutory responsibility to perform the protective functions set forth in the CIA Act of 1949.

In requesting that the Congress extend this authority to the CIA, the DNI has represented that this "arrest authority will contribute significantly to the ability of CIA protective detail personnel to fulfill their responsibility to protect officials against serious threats without being dependent on the response of federal, state, or local law enforcement officers." It is essential, in the regulations or guidelines approved by the CIA Director and the Attorney General, and in the supervision and training of protective duty personnel, that the use of the authority is firmly kept to its purpose, namely, protecting officials and any other covered persons against serious threats.

Section 422 also authorizes the CIA Director on the request of the DNI to make CIA protective detail personnel available to the DNI and to other personnel within the ODNI.

The CIA Director should provide to the congressional intelligence committees regulations or guidelines that are approved by the Director and the Attorney General. The Director should also keep the congressional intelligence committees fully and currently informed about any use of this authority.

Section 423. Technical amendments relating to titles of certain Central Intelligence Agency positions

Section 423 replaces out-of-date titles for CIA positions with the current titles of the successors of those positions in Section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q). This provision of Section 17 pertains to the obligation of the CIA Inspec-

tor General to notify the congressional intelligence committees about investigations, inspections, or audits concerning high-ranking CIA officials.

Subtitle C—Defense Intelligence Components

Section 431. Enhancement of National Security Agency training program

Section 16 of the National Security Agency Act of 1959 (50 U.S.C. 402 note) authorizes the National Security Agency (NSA) to establish an undergraduate training program to facilitate recruitment of individuals with skills critical to its mission.

Section 431 amends Section 16 to permit the NSA Director to protect intelligence sources and methods by deleting a requirement that NSA publicly identify to educational institutions students who are NSA employees or training program participants. Deletion of this disclosure requirement will enhance the ability of NSA to protect personnel and prospective personnel and to preserve the ability of training program participants to undertake future clandestine or other sensitive assignments for the Intelligence Community.

The Committee recognizes that nondisclosure is appropriate when disclosure would threaten intelligence sources or methods, would endanger the life or safety of the student, or would limit the employee's or prospective employee's ability to perform intelligence activities in the future. Notwithstanding the deletion of the disclosure requirement, the Committee expects NSA to continue to prohibit participants in the training program from engaging in any intelligence functions at the institutions they attend under the program. See H.R. Rep. No. 99–690, Part I (July 17, 1986) ("NSA employees attending an institution under the program will have no intelligence function whatever to perform at the institution.").

Section 432. Codification of authorities of National Security Agency protective personnel

Section 432 amends the National Security Agency 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 NSA.

New Section 21(a) would authorize the Director of NSA to designate NSA personnel to perform protective detail functions for the Director and other personnel of NSA who are designated from time to time by the Director 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 21(b) would provide that NSA personnel, when engaged in performing protective detail functions, and in furtherance of those functions, may exercise the same arrest authority that Section 422 provides for CIA protective detail personnel. The arrest authority for NSA protective detail personnel would be subject to guidelines approved by the Director of NSA and the Attorney General. The purpose and extent of that arrest authority, the limita-

tions on it, and reporting expectations about it are described in the section-by-section explanation for Section 422. That analysis and explanation applies equally to the arrest authority provided to NSA protective detail personnel by Section 21(b).

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

Section 433. Inspector General matters

The Inspector General Act of 1978 (Pub. L. No. 95–452 (October 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 IGs 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." 5 U.S.C. App. 2. They also perform an important reporting function, "keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of . . . programs and operations and the necessity for and progress of corrective action." Id. The investigative authorities exercised by Inspectors General, and their relative independence from the government operations they audit and investigate, provide an important mechanism to ensure that the operations of the government are conducted as efficiently and effectively as possible.

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

The National Reconnaissance Office, the Defense Intelligence Agency, the National Security Agency and the National Geospatial-Intelligence Agency have established their own "administrative" Inspectors General. However, because they are not identified in Section 8G of the Inspector General Act of 1978, they lack explicit statutory authorization to access information relevant to their audits or investigations, or to compel the production of information via subpoena. This lack of authority has impeded access to information, in particular information from contractors that is necessary for them to perform their important function. These Inspectors General also lack the indicia of independence necessary for the Government Accountability Office to recognize their annual financial statement audits as being in compliance with the Chief Financial Officers Act of 1990 (Pub. L. No. 101–576 (November 15,

1990)). The lack of independence also prevents the DoD IG, and would prevent the Inspector General of the Intelligence Community, from relying on the results of NRO, DIA, NSA, or NGA Inspector General audits or investigations 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 IGs to perform their audits and investigations, Section 433 amends Section 8G(a)(2) of the Inspector General Act of 1978 to include NRO, DIA, NSA, and NGA as "designated federal entities." As so designated, the heads of these IC elements will be required by statute to administratively appoint Inspectors General for these agencies.

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

To protect vital national security interests, Section 433 permits the Secretary of Defense, in consultation with the DNI, to prohibit the Inspectors General of the NRO, DIA, NSA, and NGA from initiating, carrying out, or completing any audit or investigation they are otherwise authorized to conduct. This authority is similar to the authority of the CIA Director under Section 17 of the CIA Act 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. It will provide the President, through the Secretary of Defense, in consultation with the DNI, a mechanism to protect extremely sensitive intelligence sources and methods or other vital national security interests. The Committee expects that this authority will be exercised rarely by the DNI or the Secretary of Defense.

Section 434. Confirmation of appointment of heads of certain components of the intelligence community

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

Section 434 provides, expressly and uniformly, that the heads of each of these entities shall be nominated by the President and that the nominations will be confirmed by the Senate. NSA, NGA, and NRO play a critical role in the national intelligence mission. Their

spending comprises a significant portion of the entire intelligence budget of the United States, and a substantial portion of the NIP. Through advice and consent, the Senate can enable the Congress to fulfill more completely its responsibility for providing oversight to the intelligence activities of the United States Government. Section 434 does not alter the role of the Committee on Armed Services in reviewing and approving the promotion or assignment of military officers.

Section 434(e) provides that the amendments made by Section 434 apply prospectively. Therefore, the Directors of NSA, NGA, and NRO on the date of the enactment of this Act will not be affected by the amendments, which will apply initially to the appointment and confirmation of their successors.

Section 435. Clarification of national security missions of National Geospatial-Intelligence Agency for analysis and dissemination of certain intelligence information

The National Imagery and Mapping Agency Act of 1996 (Pub. L. No. 104–201 (September 23, 1996) (NIMA Act)) formally merged the imagery analysis and mapping efforts of the Department of Defense and the CIA. In the NIMA Act, Congress cited a need "to provide a single agency focus for the growing number and diverse types of customers for imagery and geospatial information resources within the Government . . . to harness, leverage, and focus rapid technological developments to serve the imagery, imagery intelligence, and geospatial information customers." Section 1102(1) of the NIMA Act. Since then, there have been rapid developments in airborne and commercial imagery platforms, new imagery and geospatial phenomenology, full-motion video, and geospatial analysis tools.

Section 921 of the National Defense Authorization Act for Fiscal Year 2004 (Pub. L. No. 108–136 (November 24, 2003)) changed the name of the National Imagery and Mapping Agency to the National Geospatial-Intelligence Agency. The name change was intended to introduce the term "geospatial intelligence" to better describe the unified activities of NGA related to the "analysis and visual representation of characteristics of the earth and activity on its surface." See S. Rep. 108–46 (May 13, 2003) (accompanying The National Defense Authorization Act for Fiscal Year 2004, S. 1050, 108th Cong., 1st Sess.).

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

The Committee believes that FMV and ground-based photography should be included, with available positional data, in NGA data repositories for retrieval on Department of Defense and IC networks. Current mission planners and military personnel are

well-served with traditional imagery products and maps, but FMV of the route to and from a facility or photographs of what a facility would look like to a foot soldier—rather than from an aircraft—would be of immense value to military personnel and intelligence officers. Ground-based photography is amply available from open sources, as well as other government sources such as military units, United States embassy personnel, Defense Attachés, Special Operations Forces, foreign allies, and clandestine officers. These products should be better incorporated into NGA data holdings.

To address these concerns, Section 435 adds an additional national security mission to the responsibilities of the NGA. To fulfill this new mission, NGA would be required, as directed by the DNI, to develop a system to facilitate the analysis, dissemination, and incorporation of likenesses, videos, or presentations produced by ground-based platforms, including handheld or clandestine photography taken by or on behalf of human intelligence collection organizations or available as open-source information into the National System for Geospatial Intelligence.

Section 435 also makes clear that this new responsibility does not include the authority to manage the tasking of handheld or clandestine photography taken by or on behalf of human intelligence collection organizations. Although Section 435 does not give the NGA direct authority to set technical requirements for collection of handheld or clandestine photography, the Committee encourages the NGA to engage IC partners on these technical requirements to ensure that their output can be incorporated into the National System for Geospatial-Intelligence.

Section 435 does not modify the definition of "imagery" found in Section 467(2)(A) of Title 10, U.S.C., or alter any of the existing national security missions of the NGA. With Section 435, the Committee stresses the merits of FMV and ground-based photography and clarifies that the exclusion of "handheld or clandestine photography taken by or on behalf of human intelligence organizations" from the definition of "imagery" under the NIMA Act does not prevent the exploitation, dissemination, and archiving of that photography. In other words, NGA would still not dictate how human intelligence agencies collect such ground-based photography, have authority to modify its classification or dissemination limitations, or manage the collection requirements for such photography. Rather, NGA should simply avail itself of this ground-based photography, regardless of the source, but within the security handling guidelines consistent with the photography's classification as determined by the appropriate authority.

Subtitle D—Other Elements

Section 441. Clarification of inclusion of Coast Guard and Drug Enforcement Administration as elements of the intelligence community

Section 441 restores, with respect to the United States Coast Guard, the prior definition of "intelligence community" in the National Security Act of 1947 applicable to that service. See 50 U.S.C. 401a. Section 1073 of the Intelligence Reform Act modified the definition of "intelligence community," inadvertently limiting the Coast Guard's inclusion in the Intelligence Community to the Office of In-

telligence or those portions of the Coast Guard concerned with the analysis of intelligence. Section 441 clarifies that all of the Coast Guard's intelligence elements are included within the definition of the "intelligence community."

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

TITLE V—FOREIGN INTELLIGENCE AND INFORMATION COMMISSION

Section 501. Short Title

Title V of the bill establishes a Foreign Intelligence and Information Commission ("the Commission") to assess needs and provide recommendations to improve foreign intelligence and information collection, analysis and reporting. Section 501 provides that this title may be cited as the "Foreign Intelligence and Information Commission Act."

Section 502. Definitions

Section 502 provides definitions, including subsection 502(6) which defines "information" to include information of relevance to the foreign policy of the United States collected and conveyed through diplomatic reporting and other reporting by personnel of the Government of the United States who are not employed by an element of the Intelligence Community, including public and open-source information.

Section 503. Findings

Section 503 provides findings of Congress. Among the findings are: Accurate, timely, and comprehensive foreign intelligence and information are critical to the national security of the United States and the furtherance of the foreign policy goals of the United States; it is in the national security and foreign policy interests of the United States to ensure the global deployment of personnel of the Government of the United States who are responsible for collecting, reporting, and analyzing foreign Intelligence Information, including specifically personnel from the Intelligence Community and the Department of State, as well as other elements of the Government of the United States, and that adequate resources are committed to effect such collection, reporting and analysis.

Section 504. Establishment and functions of the Commission

Section 504 sets forth the functions of the Commission to include evaluating global strategies of the United States to collect and analyze foreign intelligence and information based on current and projected national security and foreign policy priorities; providing recommendations to improve the process for formulating such strategies; evaluating the extent to which the Government of the United States coordinates such strategies across agencies and clandestine, diplomatic, military and open-source channels; and providing recommendations to improve that coordination.

In addition, the functions of the Commission also include evaluating and providing recommendations related to the allocation of human and budgetary resources through the interagency process;

the role of country missions in the interagency process; the extent to which collection and analytic capabilities meet requirements related to strategic issues and anticipating crises or emerging threats and whether human and budgetary resources have been directed to such requirements; the role of out-of-capital embassy posts in contributing to information collection objectives; the promotion and development of language, cultural training and other relevant qualifications within the Intelligence Community and the Department of State; and the capabilities to collect and report on ungoverned and undergoverned countries and regions, terrorist safe havens, stability, radicalization, and other concerns.

Section 505. Members and staff of the Commission

Section 505 establishes that the Commission shall be composed of 14 members, to include three members appointed by the majority leader of the Senate, three members appointed by the minority leader of the Senate, three members appointed by the Speaker of the House of Representatives, three members appointed by the minority leader of the House of Representatives, one nonvoting member appointed by the Director of National Intelligence, and one nonvoting member appointed by the Secretary of State.

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

Subsection 505(b) provides for the staff of the Commission and the selection of an Executive Director.

Section 506. Powers and duties of the Commission

Section 506 provides the powers and duties of the Commission, including holding hearings, receiving evidence, and issuing and enforcement of subpoenas.

Section 507. Report of the Commission

Section 507 provides that no later than 18 months after the appointment of members, the Commission shall submit an interim report to the congressional intelligence committees. No later than 6 months thereafter, the Commission shall submit a final report to the President, the Director of National Intelligence, the Secretary of State, and the congressional intelligence committees.

Section 508. Termination

Section 508 provides that the Commission shall terminate 60 days after the submission of the Commission's final report.

Section 509. Nonapplicability of Federal Advisory Committee Act

Section 509 provides that the Federal Advisory Committee Act (5 U.S.C. App.) does not apply to the Commission.

Section 510. Funding

Section 510 authorizes that of the amounts available for the NIP for fiscal year 2009, $5,000,000 shall be available for transfer to the Commission.

TITLE VI—TECHNICAL AMENDMENTS

Section 601. Technical amendment to the Central Intelligence Agency Act of 1949

Section 601 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 602. Technical amendments relating to the multiyear National Intelligence Program

Section 602 updates references to the "multiyear national foreign intelligence program" in the National Security Act of 1947 to incorporate and reflect organizational and nomenclature changes made by the Intelligence Reform Act.

Section 603. Technical clarification of certain references to Joint Military Intelligence Program and Tactical Intelligence and Related Activities

Section 603 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 budget for the Military Intelligence Program (MIP), the successor program of the Joint Military Intelligence Program and Tactical Intelligence and Related Activities. Section 503 also preserves the requirement for consultation by the Secretary of the Defense with the DNI in the reprogramming or transfer of MIP funds.

Section 604. Technical amendments to the National Security Act of 1947

Section 604 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 605. Technical amendments to the Intelligence Reform and Terrorism Prevention Act of 2004

Section 605 makes a number of technical and conforming amendments to the Intelligence Reform Act.

Section 606. Technical amendments to the Executive Schedule

Section 606 makes technical amendments to the Executive Schedule to correct outdated and incorrect references. This section substitutes the "Director of the Central Intelligence Agency" for the previous reference in Executive Schedule Level II to the "Director of Central Intelligence." See 5 U.S.C. 5313. Section 606 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.

COMMITTEE COMMENTS

Continued misuse of supplemental budgeting process

The Committee had planned to review and recommend the authorization of supplemental appropriations to fund intelligence operations related to the conflict with al Qaeda and the continuing military operations in Iraq for the next fiscal year. However, the Administration has not yet forwarded its fiscal year 2009 supplemental appropriations request for these purposes. The Committee considers this delay unfortunate.

The Committee again notes that the Administration's request for fiscal year 2009 fails to fund all planned intelligence operations in the base budget and continues improperly to rely on supplemental appropriations requests to pay for foreseeable expenses. Although by definition, supplemental appropriations bills "are for unforeseen emergencies requiring urgent expenditures that cannot be postponed until enactment of the next regular annual appropriations act" (Congressional Quarterly, American Congressional Dictionary), fiscal year 2009 marks the eighth year that the Executive branch has requested supplemental appropriations to fund intelligence operations against al Qaeda and related terrorist groups, and the fifth year that such funding has been used to pay for IC costs in support of the conflict in Iraq.

Last year, the Administration submitted its supplemental request to pay for the Global War on Terrorism and Iraq requirements at the same time the base budget was presented to the Congress. The timing of these requests demonstrates that the Administration can budget for these efforts as part of the regular budget process, and that the costs for the effort against al Qaeda and in Iraq are not unforeseen emergencies that should be funded in supplemental bills. Nevertheless, the Administration continues to undermine the budget process by refusing to fund in its base budget request the fiscal year 2009 costs of intelligence operations in the conflict against al Qaeda and in support of military operations in Iraq.

As the Committee noted last year, the reliance on supplemental appropriations to pay for known budget expenses hinders long-term planning; causes uncertainty in all programs funded through this process; increases costs due to a reliance on contractors; and otherwise discourages fiscal discipline by presenting additional opportunities to fund questionable projects. The Committee believes the next administration should return to more sound budget practice and substantially reduce if not eliminate this reliance on supplemental funding in the future.

Information sharing and information technology

The Committee remains concerned about the status of information sharing across the Intelligence Community. The 9/11 Commission stressed the need for the IC to change information procedures to "provide incentives for sharing, to restore a better balance between security and shared knowledge." Today, at unique centers such as the National Counterterrorism Center and the National

Counter Proliferation Center intelligence information from across the IC is made available to analysts either employed by or detailed to these centers regardless of classification or compartmentation. The level of information sharing at these mission-specific centers, however, remains the exception, not the rule. Individual IC agencies still do not routinely provide other intelligence agencies broad and seamless access to the intelligence information stored within their databases. These practices limit the utility of this intelligence and prevent the establishment of a truly synergistic, collaborative intelligence environment.

Although the Committee believes the Director of National Intelligence has improved information sharing, and the Committee supports the Information Sharing Strategy issued by the DNI on February 22, 2008, the Committee believes more needs to be done and that it needs to be done more quickly. As outlined in the Information Sharing Strategy, the Chief Information Officer of the Intelligence Community (IC CIO) has taken a lead role by initiating the creation of a Single Information Environment (SIE), which will develop common email and other communications services, provide common data centers, integrate information technology (IT) communications lines, and consolidate software license purchases. While recognizing that policy issues remain to be addressed before the SIE's potential can be fully realized, the Committee believes the deployment of the SIE should be expedited. The Committee has recommended additional resources in fiscal year 2009 to enable the IC to shorten the time necessary to fully implement the SIE.

The Committee notes that initiatives similar to the SIE in the private sector have saved significant resources and improved efficiency and effectiveness. The IC to date, however, has not been able adequately to determine current expenditures within the component agencies or the financial savings that will be generated by consolidating these services, centers and networks in the implementation of the SIE. Therefore, the Committee directs the DNI to provide a report to the congressional oversight committees by February 1, 2009, identifying the resources within the individual IC programs for each IT area to be consolidated in the SIE; and estimating the savings in individual IC programs to be gained through the implementation of each of the six IT areas of the SIE.

The Committee is concerned that certain interpretations of the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. No. 108–458, December 17, 2004) (Intelligence Reform Act) and other statutes granting authorities to the DNI and the IC CIO, and bureaucratic inertia, have hampered the implementation of the SIE and other information sharing initiatives. To correct this situation, the Committee has recommended steps to withhold some enterprise IT funding from the IC agencies pending a certification by the IC CIO that individual agencies are fully implementing the SIE initiative and otherwise complying with IC CIO direction.

Information sharing and counterintelligence

The Committee recognizes that the revolution in information technology has increased the need for ensuring the security of intelligence information as well as the sources and methods used to collect that information. The spy of yesterday could steal reams of paper reports over time equal to a book's worth of information; the

spy of today in a minute could steal more than a thousand times that amount of information on a thumb drive. As the IC improves its ability to share information across agencies, the need for proper security procedures grows as well.

Although IC officials have raised the issue of security to limit access to valuable information, the Committee believes the costs of not sharing information outweigh the presumed benefits of outmoded information access policies. The same revolution in information technology that enables better information sharing also provides improved means to protect against an insider threat. The Committee has recommended increases in funding for counterintelligence and security to help ensure that improved information security proceeds at the same pace as improved information sharing.

Counterintelligence at the United States Embassy in Moscow

The Committee remains concerned about the possible counterintelligence impact of the large number of foreign national employees working at the United States Embassy in Moscow. Committee members and staff who have visited came away with a view that the State Department could do more to improve the counterintelligence posture of Embassy Moscow.

The Committee believes that this is a serious shortcoming that should be corrected on an urgent basis. The Committee encourages the Department of State to take immediate steps to improve conditions by hiring American guards to supervise the foreign national security force currently providing security.

Information security in the Intelligence Community

The Committee is concerned about potential threats to IC information systems and seeks improved accountability for IC information security. The Committee, therefore, requests that the DNI submit a report to the congressional intelligence committees, by September 1, 2008, on the following topics.

The DNI should include his interpretation of how the Federal Information Security Management Act (FISMA) of 2002 applies to the Intelligence Community and whether FISMA and the subsequent Intelligence Reform Act are properly aligned. The report should provide a comprehensive accounting of which U.S. information security standards apply to which IC information systems; the specific roles and responsibilities of the DNI for IC information security under relevant legislation, executive orders, and current practices; and the important roles and responsibilities for IC information security leadership that are not currently held by the DNI.

In addition, the report should discuss how accountability for IC information security could be improved and comment on the desirability of a community-wide, comprehensive process enabling the DNI to perform risk-need and cost-benefit analysis of potential information security initiatives such as those listed in the classified annex to accompany the classified Schedule of Authorizations.

Also, the Committee requests that the Inspectors General of the DNI and the Department of Homeland Security jointly assess sharing of U.S. cyber threat information and submit a report to the congressional intelligence committees by September 1, 2008. This assessment should focus on how cyber threat intelligence information, including classified information, is shared with the U.S. critical in-

frastructure leadership; the mechanisms by which classified cyber threat information is distributed; and the effectiveness of this threat information sharing.

Finally, the Committee requests that the DNI and the Secretary of Homeland Security perform a joint, comprehensive, up-to-date assessment of the cyber threat to U.S. critical infrastructure and submit a report on this assessment to the congressional intelligence committees by September 1, 2008. The assessment should include all types of cyber threats, of domestic or foreign origin, particularly those to U.S. electric power command and control systems.

Need for increased and stable research and development funding

The Intelligence Community has a heralded history of conceiving, developing and deploying creative and innovative technologies in support of its intelligence collection mission. In the past, the IC was recognized as being more advanced than the leading edge of private industry in developing advanced technologies. This led to such successes as the U2 and SR–71 spy planes, electro-optical satellites, and powerful supercomputers. In the past two decades, however, the advances in computer and other information technologies have been led by private industry. The IC has had to adapt in the wake of these complex and disruptive scientific breakthroughs. The Committee believes, to be successful in the future, the IC needs to not only keep up with new technologies but must lead the way in developing new sensors, analytical enablers, knowledge management tools, and other capabilities to provide the nation's policymakers and war fighters with an information advantage.

Unfortunately, the IC in recent years has sacrificed investment in tomorrow's advanced research and development (R&D) to pay for today's acquisition programs, including cost overruns and sensors of decreasing utility. Last year, in recognition of this problem, the DNI issued budget guidance to the IC agencies directing them to increase R&D spending by one percent. Despite the DNI's guidance, the Intelligence Community did not produce such budget requests. The Committee believes this short-changing of R&D must end.

Today, the Intelligence Community spends approximately three percent of its budget on research and technology. The Committee's Technical Advisory Group studied how this level compared with how private industry invested in R&D, and found that this level was significantly lower than companies in the automobile, energy and IT industries spend on the same function. While not being able to determine analytically the right level, the TAG found that the IC's current level of R&D investment was on its face too low given the challenges the IC faces both today and in the future.

As a result, the Committee has recommended significant changes to the budget request to follow the DNI's direction and increase R&D spending in the IC to 4 percent of its total budget in fiscal year 2009. Further, the Committee believes the IC needs to gradually increase its R&D spending to at least five percent to address future collection and analysis requirements. The Committee plans to recommend such growth in future authorization bills and to keep this funding stable to ensure the United States will be able to develop the next generation of sensors and systems to prevent attacks and strategic surprise.

FBI intelligence transformation

The Committee has spent considerable time examining the efforts of the Federal Bureau of Investigation (FBI) to transform itself into a premier intelligence and national security organization. This has included briefings with current and former FBI officials, oversight visits to FBI field offices and Legal Attaches, meetings with representatives of other intelligence agencies regarding FBI transformation efforts, and exchanges with academics and think tank experts on the structure and functions of FBI national security components. Additionally, in October of 2007, the Committee held an open hearing with the Chairman and Vice Chairman of the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission), who provided their assessment of FBI intelligence reform efforts.

The Committee has come to the conclusion that the FBI must work harder and faster if it is to fulfill its national security and intelligence mission. Nearly seven years after the attacks of September 11, 2001, the FBI has yet to make the dramatic leaps necessary to address the threats facing our nation. The Committee has identified several areas where the FBI must focus to improve its mission performance and accelerate its reform efforts.

As set forth in Section 333, the bill requires the Director of National Intelligence, in coordination with the Director of the FBI, to establish performance metrics and specific timetables related to progress in the areas outlined below. Additionally, the DNI is to submit a consolidated semi-annual report, which includes an assessment of the metrics, timetables, corrective actions, and activities being carried out to ensure that the FBI is improving its national security and intelligence mission performance. The report should be provided to the congressional intelligence committees semi-annually for a period of five years beginning on the date of enactment.

The Committee stands ready to assist the FBI in its transformation efforts, but notes that the FBI must improve its cooperation and transparency with Committee oversight activities. Too often the FBI has not cooperated in a manner as the Committee would have expected to Committee requests for information related to its intelligence and national security programs.

FBI and ODNI engagement

The Committee believes additional cooperation between the Office of the Director of National Intelligence and the FBI is a prerequisite to successful FBI intelligence reform. The White House memorandum that established the FBI's National Security Branch (NSB) in 2005 stated that the DNI must concur with the FBI's nomination for the Executive Assistant Director of the NSB and that the Attorney General and the DNI must establish procedures to ensure the DNI can effectively "communicate" with FBI field offices and personnel. The Committee believes this does not go far enough and that the ODNI may require additional authorities to direct and manage the FBI's intelligence programs.

Specifically, the Committee believes the ODNI should examine and address the FBI's NIP budget structure, intelligence enabling IT programs, efforts to advance an analytic culture, intelligence training curriculum, and the ability of the NSB to manage and di-

rect intelligence programs enterprise wide. The Committee requests the ODNI focus on these efforts, and any others meant to strengthen FBI mission performance on national security and intelligence matters.

FBI and the National Intelligence Program budget structure

The Committee's oversight of FBI budget matters has been impaired by the agreement reached by the previous DNI and the previous Attorney General on which elements of the FBI fall within the NIP. The agreement was an artificial construct intended to keep the FBI NIP numbers stable, and has had the detrimental effect of making it nearly impossible to track NIP resources accurately within the FBI. The agreement involves calculating varying percentages of agents, analysts, and infrastructure, and is so complicated that the proposed addition of funds to the FBI budget by the congressional appropriations committees required help from the DNI's Chief Financial Officer to parse how much of that funding was within the NIP. The FBI itself had such difficulty calculating the correct number of agents for the fiscal year 2007 budget request that it had to issue an errata sheet to the NIP Congressional Justification Book.

At any given time, neither the Executive branch nor the Congress is able to calculate which FBI agents, analysts or IT systems are NIP-funded. Even more troubling, the Executive branch and Congress are unable to track whether NIP dollars are being expended and accounted for as they are authorized and appropriated. The Committee believes this unworkable arrangement must end and that the entire FBI NSB should be NIP funded. Auxiliary administrative services that support both the NSB and the rest of the FBI should be billed to the NSB and reimbursed with NIP funds. The ODNI and FBI should fully fund the NSB under the NIP in fiscal year 2010.

FBI and intelligence enabling information technology

The Committee has had long-standing concerns about the FBI's management and execution of information technology projects that support and enhance the FBI's national security mission. These concerns include the lack of Internet access for special agents and intelligence analysts at their desktops, an underdeveloped case management system that is restricted to SECRET level information, and the slow expansion of the FBI's separate Top Secret/Sensitive Compartmented Information (TS/SCI) level SCION data system.

The Committee's October 2007 oversight hearing found that only a third of special agents and intelligence analysts have access to the Internet at their desktops. The Committee believes it is essential that NSB personnel have easy access to open source data available on the Internet and finds the FBI's lack of progress in expanding Internet access unacceptable.

While it may not be necessary to provide Internet access to every individual FBI employee, the Internet's value as a basic research tool has been amply demonstrated, and the Committee believes that all intelligence analysts, intelligence professionals, and special agents within the FBI's National Security Branch should have desktop Internet access.

The Committee is recommending a substantial increase in resources in the classified annex to this Act to expand desktop access to a larger number of NSB personnel.

Likewise, the Committee remains concerned that the FBI lacks an IT system that can manage FBI case and document files, as well as enable the storage, analysis, and dissemination of foreign and domestic intelligence. In 2005, after spending $170 million, the FBI was forced to cancel an IT system called Virtual Case File. In its place, the FBI has begun to implement a $425 million system called SENTINEL, which will not be fully operational until 2010. At this moment, the FBI still lacks the ability to store and share images and audio files associated with its intelligence investigations. Furthermore, the Committee is concerned that SENTINEL is limited to SECRET information, preventing the integration, analysis, and dissemination of IC information that is classified at the TS/SCI level.

As a full member of the Intelligence Community, the FBI must have an intelligence information infrastructure that can receive, process, analyze, and disseminate TS/SCI material. This system should be available to every FBI field office and Legal Attaché. The FBI's Secure Work Environment initiative is an effort to construct Sensitive Compartmented Information Facilities (SCIFs) that would allow for the deployment of the FBI's TS/SCI information technology system called SCION. The FBI's national security workforce requires SCION, and a TS/SCI work environment, to effectively complete its mission. Yet, according to FBI projections, by the end of 2009, 28 percent of the targeted TS/SCI connectivity will not yet be deployed. The Committee finds this lack of TS/SCI connectivity unacceptable.

Given these concerns, the Committee has been especially disappointed with the FBI's lack of transparency related to the development and deployment of its intelligence-related IT infrastructure. The Committee requested several unclassified assessments related to the SENTINEL program more than a year ago, but the FBI has refused to share these reports with the Committee. Moreover, the Committee has yet to receive follow-up reports detailing the expansion rate of SCIFs, which enable deployment of the TS/SCI information system. The Committee believes the ODNI and FBI must obtain an independent assessment of the current FBI information technology infrastructure, to include recommendations on what systems may need to be developed to support the FBI's national security mission. The Committee expects this report to be shared with congressional oversight committees as soon as it is completed.

Advancement of the FBI analytic culture

At the Committee's October 2007 FBI oversight hearing, the Chairman and Vice Chairman of the National Commission on Terrorist Attacks Upon the United States provided their assessment of current FBI reform efforts. The Commissioners stated that: (1) FBI intelligence reform required robust oversight by the congressional intelligence committees; and (2) the role of intelligence analysts at the FBI must change dramatically. The Committee agrees.

Although the number of intelligence analysts has doubled at the FBI since 2002, the FBI continues to face difficulties in training, managing, and retaining analysts.

Training: Despite "revamping" intelligence analyst training almost every year since 2002, the FBI has failed to implement an effective training program. The FBI is currently engaged in "revamping" its analyst training once again. The latest training plan is a drastic change from past intelligence analyst training programs, yet the FBI has received little to no guidance from the ODNI. Considering the FBI's repeated failures to construct a successful intelligence analyst training course, the Committee finds the lack of ODNI guidance and assistance unacceptable.

Management: The majority of intelligence analysts at the FBI are directly supervised by special agents who have little or no experience conducting intelligence analysis. An April 2007 Department of Justice (DOJ) IG report found that a strong professional divide between analysts and special agents remains, impeding the collaboration needed to meet effectively the FBI's national security mission. The FBI's response at the October 2007 hearing that the cultural divide identified by the IG report is "anecdotal," does not comfort the Committee. Moreover, the Committee does not believe FBI efforts to create a "Managing Analysis Course" for non-analysts is the appropriate response to the problems facing the FBI in this area.

Retention: The FBI still lacks a robust intelligence analyst career path. The development of such a career path began in 2003 and continues to be a work in progress. The Committee believes there are too few intelligence analysts in senior positions of responsibility and that the FBI has neglected opportunities to utilize intelligence analysts to fill inherently non-law enforcement, intelligence-focused positions. For example, few Field Intelligence Groups are led by non-special agent personnel. The FBI was granted the authority in the Consolidated Appropriations Act of 2005 to utilize critical pay authority to obtain 24 Senior Intelligence Officer (SIO) positions portrayed as "critical to the FBI's intelligence mission." In testimony to this Committee on January 25, 2007, the FBI described these SIOs as "a cadre of senior analysts who will sustain the focus on issues about which policy makers and planners need information now." As of early 2008, the FBI has hired only 2 SIOs.

The Committee has been impressed with the caliber of recently hired intelligence analysts. Many of these analysts have advanced degrees critical to the FBI's national security mission. As these new hires have entered the analyst workforce, their presence has highlighted the differences in skill sets among the FBI analytic community. A third of all intelligence analysts at the FBI were hired before the September 11, 2001 attacks. Eighty percent of those intelligence analysts were promoted into intelligence analyst positions from clerical support positions. An FBI study in 2002 found that 66% of the FBI's analysts were "unqualified" to do their work. The diversity in skill sets has caused tension within the FBI and inhibited the advancement of the FBI analytical community. The Committee believes the FBI must take steps to deal with the vast discrepancy in analyst abilities.

The Committee also believes the FBI should do more to advance the growth of its non-agent intelligence cadre and instructs the FBI to be more strategic in its deployment and use of special agents. Furthermore, the Committee instructs the FBI to continue the data collection begun by the IG of the Department of Justice to examine

FBI efforts to hire, train, and retain intelligence analysts. Finally, the Committee directs the ODNI to engage the FBI on the training, management, and retention of the FBI intelligence analyst workforce by establishing a baseline for intelligence analyst performance and assisting in the creation of benchmarks and timelines for these reforms.

FBI intelligence training curriculum

The Committee believes the ODNI is uniquely positioned to assist the FBI in creating and measuring the effectiveness of the FBI's national security and intelligence training programs.

The Department of Justice Inspector General has released several reports detailing "widespread and serious misuse" of the FBI's National Security Letter (NSL) authorities. The IG reports did not find intentional misuse of authorities, but rather that poor training, oversight, and guidance contributed to the misuse of NSL authorities. The most recent DOJ IG report indicated that the FBI has made progress in these areas. The Committee believes that continued and robust training is necessary to ensure FBI personnel are safe-guarding American civil liberties, while utilizing all legal investigative tools to protect the nation.

The Committee is also concerned about the lack of training provided to Joint Terrorism Task Force (JTTFs) members. According to information provided to the Committee, JTTF members receive "on-the-job" training that is augmented by Internet-based instruction. Considering the importance and complexity of the counterterrorism work conducted by JTTF officers, the Committee expects the FBI to develop a more demanding and structured training program that will equip JTTF members with the skills necessary to address the evolving threats from terrorism.

The Committee is also concerned about the quality of the FBI's Domestic HUMINT Collection Course (DHCC). Although the course has received a contingent certification of endorsement from the ODNI, the Committee's HUMINT study group has criticized the DHCC for its low production rates, brevity, and general lack of rigor compared to other Intelligence Community HUMINT courses.

Finally, the FBI's failure to create an effective intelligence analyst training course, referenced earlier in this report, has been an ongoing disappointment. The Committee strongly supports efforts by the FBI to properly train its workforce to ensure FBI personnel (and those detailees operating under FBI authorities) are equipped to utilize all legal investigative tools to protect the nation, while respecting and safe-guarding American civil liberties. The Committee believes the FBI will benefit substantially from ODNI guidance and assistance in creating and implementing effective intelligence and national security-related training programs.

Regionalization of the FBI Intelligence Program

From an intelligence collection, analysis, management, and dissemination perspective, the Committee believes the current FBI intelligence management model is dramatically ineffective in supervising and managing intelligence and national security programs in FBI field offices. Field Intelligence Groups (FIGs), located in each of the FBI's 56 field offices, were established in 2003 to integrate the "intelligence cycle" into FBI field operations and manage the

Field Office Intelligence Program. The Directorate of Intelligence, located within the National Security Branch of FBI headquarters, has been responsible for FIG management. Committee oversight activities, as well as internal and external consultancies, have found this management model to be ineffective. FIGs lack clear guidance, are poorly staffed, are led overwhelmingly by special agents, and are often "surged" to other FBI priorities. Moreover, the current management model has failed to link neighboring FIGs or promote larger regional analysis of trends and vulnerabilities.

The Committee believes a regionalized intelligence and national security program would allow the Bureau to more effectively track and manage trends across the United States by creating an intelligence and national security reporting chain that is more manageable and accountable. The Committee believes such a model would allow the Director of the FBI and the Director of National Intelligence to more effectively and efficiently manage FBI intelligence and national security programs.

The Committee expects the FBI to brief the Committee regularly on its efforts to regionalize the management of its intelligence and national security programs.

FBI's Weapons of Mass Destruction Directorate

The Committee believes one of the gravest threats facing our nation is the threat from weapons of mass destruction (WMD). Unfortunately, the Weapons of Mass Destruction Directorate (WMDD) within the FBI is poorly positioned to work across FBI programs that are likely to encounter WMD threats and investigations. The Committee has yet to be provided with information on how activities of the WMDD are de-conflicted with other operational and analytical divisions. Accordingly, the Committee believes the FBI must clarify the role of the Directorate in relation to other FBI components. Additionally, the Committee directs the FBI to complete a report on the impact of eliminating the WMDD investigative functions and repositioning the WMDD as an organization that collects intelligence, conducts outreach, and offers specialized support to all operational divisions of the FBI. This report should be submitted to the congressional intelligence committees no later than November 1, 2008.

FBI National Security Workforce Management

The Committee is concerned about the FBI's continued reliance on special agents to fill all types of positions. Substantial resources are devoted to providing Special Agents with unique skills and their appointments should be made in a manner that is effective and efficient. The Committee believes the use of special agents in organizational support functions unrelated to intelligence or law enforcement should be limited. Moreover, while special agents assigned to the intelligence career track should continue to compete for intelligence-focused positions, the FBI should do more to encourage the growth of its non-agent intelligence professionals. This is not only cost-effective, but allows for better strategic positioning of the FBI national security workforce. Accordingly, the Committee directs the FBI to provide the congressional oversight committees with a plan to recapture and redirect special agents to mission critical areas by identifying job roles currently performed by special

agents that could be shifted to intelligence analysts or other professional support. This plan should be submitted to the congressional intelligence committees no later than November 1, 2008.

FBI headquarters staffing of National Security Programs

The FBI has struggled to staff key national security and intelligence positions at FBI headquarters. In March 2007, only 60 percent of the Counterterrorism supervisory special agent positions were filled. In the headquarters section that covers al-Qa'ida-related cases, more than 23 percent of the supervisory special agent positions were vacant. More recently, in September 2007, Director Mueller touted a new Desk Officer Program before the Senate Committee on Homeland Security and Governmental Affairs. Director Mueller stated that desk officers identify collection gaps; collaborate with partners; and focus not only on the management and advancement of existing cases, but also on maintaining a networked and coordinated national collection effort. Yet, according to information received by the Committee, the FBI has been unable to find applicants willing to apply for the 20 desk officer special agent positions. The FBI has attempted to address headquarters vacancies by offering 18-month temporary duty assignments (TDYs) and significant monetary bonuses, but these incentives have failed to significantly change the position vacancy rates in critical FBI national security and intelligence areas. The Committee expects the FBI to engage in a credible study to identify why it has been unable to attract personnel to headquarters for mission critical areas and to develop a plan to address permanently the high position vacancy rates in its national security and intelligence programs at FBI headquarters.

The Inspector General of the Central Intelligence Agency

The CIA's Office of Inspector General serves a critical internal oversight function. As outlined in the Central Intelligence Agency Inspector General Act, 50 U.S.C. 403q, the CIA Inspector General has the responsibility for conducting independent inspections, investigations, and audits of CIA activities and operations to ensure that they are being conducted efficiently and in accordance with applicable law and regulations. By identifying problems and deficiencies and recommending corrective action to the Director, the Inspector General helps to improve the effectiveness and management of such programs. This internal oversight function is particularly important because the CIA's programs and operations are, by necessity, conducted largely in secret.

Because the Inspector General has the obligation to report to the congressional intelligence committees about problems or deficiencies in CIA programs or operations, the CIA's Office of the Inspector General serves a vital role in facilitating effective congressional oversight of the CIA. As such, the Committee has a strong interest in preserving the independence and operational autonomy of the CIA's Inspector General and in ensuring that the CIA Inspector General can operate without fear of improper intervention or intimidation.

In the spring of 2007, the Director of the CIA initiated a management review of the Office of the Inspector General. The Director stated that this review, conducted by a team within the CIA but

outside the CIA's Office of the Inspector General, was necessary to address concerns arising from two reports prepared by the Office of the Inspector General. At the conclusion of the review in January 2008, the review team presented the CIA's Inspector General with a number of recommendations for the Office of Inspector General, some of which the Inspector General agreed to implement. The CIA Director subsequently sent out a message to the CIA workforce informing them of the initiation and resolution of the review, and describing steps taken by the CIA's Inspector General based on the review.

The Committee is concerned that the Director's initiation of a review of the Office of the Inspector General could have been perceived by the CIA workforce and the public as an attempt to undermine the credibility of the Inspector General. The Committee recognizes that the applicable statute provides that the Inspector General "shall report directly to and be under the general supervision of the [CIA] Director." Because the Inspector General has a critical role in effective congressional oversight, the Committee believes that the due care should be taken to ensure, in carrying out this authority, that the independence of the office is protected. Informing the congressional intelligence committees and seeking the assistance of an outside review organization, such as the President's Council on Integrity and Efficiency, rather than initiating a unilateral internal inquiry, could have helped alleviate such concerns.

The Director's review of the CIA Office of the Inspector General highlights the possible need for additional legislative protections to safeguard the independence of the CIA Inspector General. The Committee therefore plans to study carefully the provisions of S. 2324, the Inspector General Reform Act of 2007, to determine whether any of the provisions included in that Act should be added to the CIA Inspector General Act to strengthen the authorities of the CIA Inspector General.

CIA Lessons Learned Program

The Committee commends the CIA for establishing a Lessons Learned Program and fully supports its growth at the operational and tactical level with the individual components of the CIA. The Committee firmly believes that for the CIA to truly become a learning organization—one in which knowledge is captured, preserved, and shared with those who can benefit—the CIA must institutionalize the lessons learned process and develop policy supporting that effort.

The Committee encourages the CIA to increase the number and type of studies, to create web-based lesson-sharing environments, to modernize its oral history programs and to support component-based lessons learned activities throughout the CIA. Additional lessons learned subject matter experts should be hired as well as additional officers to enable the CIA to conduct interviews to record the insights of officers in key positions as they rotate on to new assignments or move into retirement. The CIA should use these interviews as well as historical and archival research to conduct lessons learned studies and incorporate these back into the CIA education and work environments.

The Committee fully expects the CIA to improve its internal processes for self-examination, including increasing the use of for-

mal lessons learned studies to learn from its successes and mistakes and to anticipate and be ready for new challenges. The CIA should follow the lead of other high risk, high reliability organizations by investing time and resources in continuous learning and knowledge sharing. This will strengthen the professionalism and confidence of not only the CIA's new hires, but the entire CIA workforce.

National Application Office of the Department of Homeland Security

The Committee has been closely following the development of the National Application Office (NAO) within the Department of Homeland Security. The NAO is intended to centralize and facilitate the sharing of imagery from intelligence agency systems under appropriate circumstances for purposes related to law enforcement, homeland security, and civil applications. Because the NAO relates to the use of intelligence resources for domestic purposes, the Congress has been attentive to civil liberties and privacy concerns associated with the NAO.

Section 525 of the 2008 Department of Homeland Security Appropriations Act stated that "none of the funds provided in this Act shall be available to commence operations of the National Applications Office . . . until the Secretary certifies that th[is] program[ ] compl[ies] with all existing laws, including all applicable privacy and civil liberties standards, and that certification is reviewed by the Government Accountability Office." Although the Government Accountability Office (GAO) has not conducted a review of this certification, the Secretary of Homeland Security has informed Congress that he has "determined that the standard set forth in Section 525 . . . is met" thereby certifying that the NAO complies with all existing laws, including all applicable privacy and civil liberties standards, with respect to its planned operations in what are known as the civil application and homeland security domains.

The Committee, however, has not been provided the legal framework or the standard operating procedures for the use of these resources in the law enforcement domain. The Committee concurs with the decision that the NAO should proceed pending the GAO review of the certification; however, the Committee strongly opposes the NAO fielding any law enforcement requests until the legal framework and standard operating procedures of the law enforcement domain are completed, certified by the Secretary, reviewed by the GAO, and provided to the appropriate congressional oversight committees.

The Department of Homeland Security and state and local fusion centers

The purpose of state and local fusion centers is to provide state and local officials with situational awareness, threat information and intelligence on a continuous basis. The Committee notes a review by the Congressional Research Service, which found that "there is no-model for how a [fusion] center should be constructed" and that the fusion centers "have increasingly gravitated toward an all-crimes and even broader all-hazard approach."

Therefore, the Committee requests that the Secretary of the Department of Homeland Security complete a formal national fusion

center strategy outlining the federal government's clear expectations of fusion centers, its position on how federal funding will be sustained over time, and metrics for assessing fusion center performance.

Intelligence Advanced Research Projects Activity

The Committee wishes to ensure that the Intelligence Advanced Research Projects Activity (IARPA) has the appropriate authorities and stature to be effective in fulfilling its unique intelligence community mission. The Committee therefore requests that the DNI submit a comprehensive report to the congressional intelligence committees by September 1, 2008, that addresses the following topics.

The DNI should address the desirability of creating IARPA and the position of the IARPA Director formally in statute; the rationale for placing IARPA within the DNI's acquisition directorate; and the desirability of streamlining the IARPA reporting chain such that the IARPA Director reports directly to the DNI's Director for Science & Technology and this official reports directly to the DNI. In addition, the report should address the timeline for the DNI to approve the delegation of personnel and contracting authorities to the IARPA Director; any issues that would prevent the delegation of such authorities; and the desirability of authorizing this delegation of authorities formally in legislation.

The Committee is interested in the DNI's views on authorizing the IARPA Director to employ highly qualified scientific experts and to use any other staffing mechanisms to support the unique mission of IARPA; delegating to the IARPA Director existing authorities to conduct streamlined acquisition, procurement, and contracting in support of IARPA needs; authorizing the IARPA Director to give grants, awards, or prizes to support IARPA research and development programs, grand challenges or related projects; and any other authorities that could improve the flexibility or effectiveness of IARPA.

International Traffic in Arms Regulations

The Committee is concerned about the potential unintended consequences of the International Traffic in Arms Regulations (ITAR). The United States currently maintains a lead in many advanced aerospace technologies, but that lead is slipping or has already passed. Alleged foreign frustrations with ITAR are, in some cases, leading foreign governments to subsidize "cottage" industries to provide alternative sources of ITAR-restricted technologies.

In 2006, 21 European countries and Canada endorsed the research agenda of the European Space Technology Platform (ESTP). Among the many goals of the ESTP are to "reduce European dependence" on foreign space technology and to "promote the worldwide competitiveness of the European industrial base." A press release cited the ESTP stakeholders sharing views on the need to invest in "ITAR-free technologies."

A former head of the Defense Threat Reduction Agency was cited in a February 26, 2007, Space News article as saying the rules restricting the export of U.S. satellites and components "need a thorough overhaul because they are damaging U.S. industry with no corresponding benefit to national security." The Committee does

not debate the intent of ITAR, but is concerned about its unintended consequences which may be detrimental to our national security.

The U.S. no longer holds monopolies on many advanced aerospace technologies. If U.S. companies cannot compete freely in the global market and are challenged by foreign-subsidized firms with newer, and perhaps better, technologies, the end result may be that U.S. firms will go out of business or decide no longer to produce these niche technologies. In turn, this could result in further erosion of the U.S. technological lead, increased U.S. reliance on foreign suppliers for the same technologies the U.S. currently restricts, potentially unrestricted sales of advanced technologies from these same foreign suppliers to nations hostile to the U.S., and U.S. job loss.

The Committee recognizes that it is difficult to quantify ITAR's real impact on U.S. industry, and that ITAR may often be cited as the "scapegoat" for industry's troubles. Further, the Committee recognizes that if certain ITAR provisions were loosened or streamlined there would be an increased risk of proliferation of advanced technologies into the wrong hands. However, ITAR's net effect on the U.S. aerospace industry may, in the long run, be more damaging to national security.

The Committee requests that the DNI and the Secretary of Defense charter an independent, objective review of this issue to be delivered to the Congress no later than July 1, 2009. The report should evaluate the impact of ITAR on the U.S. aerospace industry, gauge the degree to which ITAR spurs foreign nations to develop indigenous aerospace technologies, assess the proliferation risks of modifying ITAR restrictions, and provide recommendations on improving ITAR's aerospace-related processes to achieve a better balance between promoting U.S. aerospace technology and discouraging the proliferation of this technology to other countries.

National Geospatial-Intelligence Agency mission

The Committee finds that strong functional management of the IC and the Department of Defense geospatial intelligence enterprise remains wanting. Significant gaps remain in the integration of airborne, commercial, and non-traditional imagery; new geospatial-related capabilities are being under-resourced or provided little architectural construct against which to plan; the overall architecture contains imbalances between the sensors and their supporting tasking, processing, exploitation, and dissemination (TPED) systems; and imagery-related investments are being driven by disparate agencies with little consideration of efficiencies in the overall architecture. These problems have resulted in excessive costs; poor interoperability; costly "crash" TPED programs for systems already in operation; and lost opportunities to invest in new capabilities.

The inability of the former Central Imagery Office to influence budgets and enforce policy was often cited as the rationale for creating a more powerful imagery authority. Consistent with the recommendations of the 1992 Report Regarding Restructuring the Imagery Community, also known as the Burnett Panel report, the creation of the National Imagery and Mapping Agency (NIMA)—predecessor to the National Geospatial-Intelligence Agency—was large-

ly intended to address functional management problems. The National Imagery and Mapping Agency Act of 1996 (Pub. L. 104–201) intended the NIMA to "provide a single agency focus for the growing number and diverse types of customers for imagery and geospatial information resources within the government, to ensure visibility and accountability for those resources, and to harness, leverage, and focus rapid technological developments to serve the imagery, imagery intelligence, and geospatial information customers." The Committee finds, however, that the creation of NIMA has only marginally helped the government achieve these goals.

The NIMA, and later the NGA, have made significant strides in managing traditional national imagery activities, for which they deserve praise. Furthermore, the current NGA leadership has notably increased its functional management efforts. However, despite significant increases to its budget, the NGA has inadequately managed the rapid developments in advanced geospatial intelligence, and airborne and ground-based imagery collection systems. For example, the acquisition of imagery-related unmanned aerial vehicles lacked coherent central guidance, resulting in disparate, incompatible, and "stovepiped" systems; current decisions regarding new imagery satellite programs have lacked strong NGA input; costly classified sensors were procured without adequate TPED; and no system exists to store ground-based imagery.

The need for management of the nation's geospatial enterprise, not shortcomings in analysis, was the driving rationale for creating the NIMA. The Burnett Panel noted a need to centralize vital functions such as end-to-end planning/management, research and development, collection, processing, archiving, and infrastructure, while maintaining the distributed nature of the imagery exploitation process to best support the all-source intelligence agencies. The Committee concurs, believing that enabling use of geospatial intelligence by all customers should be a key goal of NGA's functional management efforts.

The Committee believes that the NGA possesses a strong analysis and production culture, inherited from predecessor organizations which formed the NIMA, but a strong functional management culture must be further developed. Indeed, the Committee is concerned that since the NIMA's creation, there has been a net consolidation of analysis without sufficient improvements to functional management.

As a case in point, the NGA objected to legislation requiring the development of a system to facilitate the analysis, dissemination, and incorporation of imagery collected by ground-based platforms. Ground-based photography of known sites and routes is now commonplace—enabled even by cell phones with photographic capability—and of great use to military personnel or clandestine operatives. Despite NGA's claims that it has the needed authorities to mandate such a system, no such system exists. Furthermore, NGA personnel have stated there is no need for such a system because the data is of little use to NGA analysts. This view may explain the poor performance in establishing architectural guidance for airborne systems as well, since NGA analysts overwhelmingly rely on satellite imagery. The Committee stresses that the NGA, in its role as functional manager, must respond to the needs of all users of geospatial information, not just NGA analysts.

The NGA, like the NIMA before it, is granted by statute, Defence Department Directives, and Intelligence Community Directives significant authorities over geospatial intelligence activities. Despite this, the NGA Director's ability to influence the geospatial-related investments of non-NGA entities is limited. Like the former Central Imagery Office, the NGA lacks the ability to enforce its policies and standards outside the agency, yet NGA management states that they need no stronger authorities.

Since the creation of NIMA, two new positions—the Director of National Intelligence and the Undersecretary of Defense for Intelligence—have been established, both with certain authorities which may supplant those of the NGA. The Committee believes that the geospatial intelligence functional management authorities of the NGA should be reviewed in light of this new IC leadership. If strong central leadership is needed, then more powerful and clear authorities should be delegated to the organization entrusted with that role. The Committee encourages the NGA to review what was the founding rationale and intent for the NIMA, and ensure that the agency's focus is consistent with that intent. Further, the Committee encourages the DNI, Secretary of Defense, and Secretary of Homeland Security to review the geospatial intelligence management issue, delineate appropriate responsibilities and authorities, and then ensure that those responsibilities are met.

Resolution restrictions on commercial imagery satellites

The national defense and intelligence communities rely on commercial satellite imagery for many missions. The Committee believes it is in the national interest to maintain U.S. leadership in this field, including a regulatory regime that is balanced between protecting national security and allowing a competitive U.S. industry.

The 2003 U.S. Commercial Remote Sensing Policy directs the U.S. Government to "rely to the maximum practical extent" on commercial imagery providers, with a goal of "maintaining the nation's leadership in remote sensing space activities." It also advises Government agencies to provide a "responsive regulatory environment for licensing the operations . . . of commercial remote sensing space systems."

There is an increasing rationale to use commercial systems for more complex national security missions. Likewise, there is a growing commercial marketplace for higher-resolution imagery. While market conditions demand higher quality imagery, foreign competition is aggressively investing in more advanced imaging capabilities, and quickly closing the technology gap between themselves and U.S. providers.

A number of foreign commercial systems—either already on orbit, or scheduled for launch in the next few years—provide comparable resolution to current U.S. commercial satellites, which is limited by U.S. policy. The Committee understands that the factors governing U.S. policies in this area include complex trade-offs. However, it appears obvious that the U.S. no longer holds a monopoly on satellite imagery.

Satellite acquisitions take at least three years from contracting to launch. In order for our commercial imagery providers to maintain their competitiveness, they must be able to anticipate relaxed

resolution restrictions several years in advance. A review of current policy restrictions with an eye toward more relaxed licensing agreements in the 2010 to 2011 timeframe could allow commercial industry to procure more capable systems.

The Committee encourages the harmonization of U.S. government regulations governing commercial remote sensing satellite imagery with the imagery needs of the defense and intelligence communities consistent with national policy and prudent risk management. Therefore, the Committee directs the DNI, in coordination with the Departments of Defense and Commerce, to review ground sampling distance licensing restrictions for U.S. commercial remote sensing space systems.

INTELLIGENCE COMMUNITY FINANCIAL MANAGEMENT

The Senate Select Committee on Intelligence formally began its quest for increased IC compliance with federal financial accounting standards in September 2001. The report language accompanying the Committee's Fiscal Year 2002 Intelligence authorization bill noted that as early as January 1997 the President had called for selected IC agencies to begin producing classified financial statements. The report language called for the financial statements of the National Reconnaissance Office (NRO), the National Security Agency (NSA), the CIA, the Defense Intelligence Agency (DIA), and what is now the NGA to be audited by a statutory IG or independent public accounting firm by March 1, 2005. The intent was that by this time, the statements would be auditable.

Since September 2001 each agency has overstated its progress in establishing the processes, procedures, and internal controls that would allow for the production of auditable financial statements. These promises have been accompanied by the hiring of multiple contractors who have created numerous studies and plans that have often been duplicative and merely pointed out the obvious. There has also been an apparent lack of senior management attention to the need for improved financial accountability. This lack of attention was most recently exhibited when the directors of the five agencies mentioned above were asked to respond to questions raised concerning the Annual Financial Report submitted by their agency in November 2007. The response from the NSA was the only one signed by the director of the agency, and the CIA submitted its response over one week late with no explanation. The agency responses generally addressed the issues raised, but each lacked details on when critical corrective processes or new systems would be implemented while promising to be auditable by the DNI imposed deadline of 2012. Based on past history, the Committee is hesitant to accept these promises.

The Committee acknowledges that there has been nominal progress over the last decade. The NRO produced an auditable financial statement in fiscal year 2003, but since then has slipped to the point of not doing an audit of its fiscal year 2007 statement pending further improvements to internal processes. The NSA has implemented a new financial management system that will also support the DIA, and the CIA continues to upgrade its core financial system. The NGA, on the other hand, has still not begun implementation of a core financial system, and is the farthest from producing auditable financial data. Additionally, much of the

progress to date is offset by the reliance on inadequate feeder systems and intensive manual processes to create the actual statements. The bottom line is that over ten years after the President called for action, and over three years after the Committee anticipated receiving auditable statements, the five agencies are still unable to produce an auditable financial statement and the current projection for doing so is at least four years away.

The current plan for producing auditable statements is contained in an April 2007 DNI report titled: Financial Statement Auditability Plan. The report outlined the current state of the intelligence community's financial management systems, explained the challenges to achieving unqualified audit opinions, and specified key milestones for each agency on the path to clean audit opinions in fiscal year 2012. The report failed, however, to explain how independent audit assessments of important milestones would be conducted, and it contained no plan for when individual systems could be merged into a business enterprise architecture (BEA). The Committee had originally asked the DNI for a plan to create such an architecture in December 2006. Also, based on the Committee's research with private sector experts and a review of best practices elsewhere in the U.S. Government, the Committee was concerned that the approach outlined in the April 2007 report rested too heavily on past decisions and sunk costs of the individual agencies, and did not fully embrace the shared service model endorsed by the Office of Management and Budget. Finally, the Committee was concerned that the proposal for clean audit opinions by 2012 did not convey a sense of urgency.

The Committee was particularly interested in the ODNI producing the follow-on study referenced in the April 2007 report. The follow-on study was to include a determination on the feasibility of incorporating the IC's financial management domain into a BEA. Report language that accompanied the Committee's fiscal year 2008 intelligence authorization bill specifically requested that the follow-on study include an impartial evaluation of the following: DNI authorities to enforce compliance with federal financial accounting standards; the most cost effective system solution and the responsibilities of the Intelligence Community's Chief Information Officer in overseeing pursuit of that solution; and the findings of recent IC information technology assessments and IG reports.

The Committee originally intended for the results of the follow-on study to be received by December 1, 2007, but after further discussion with industry experts and the House Permanent Select Committee on Intelligence, the report due date was deferred until March 31, 2008, to allow for the creation of a meaningful product. Ultimately, the report was received nearly two weeks late and failed to cover a number of issues requested by the Committee. The report proposes to address many of the most critical issues in a separate report to be produced by September 30, 2008. While the turnover of senior financial personnel within the ODNI delayed production of the report, it is clear that the task received inadequate attention during the time available. More importantly, the lack of action further delays meaningful independent oversight of the efforts of the agencies to achieve auditable financial statements.

While the Committee is resigned to allowing the DNI's new financial managers time to produce the required solutions to the IC's financial accountability issues, it can no longer wait for meaningful independent confirmation that the current actions of the agencies will lead to the internal controls necessary to produce auditable financial statements. Therefore, the Committee directs the DNI to submit a proposal by December 1, 2008, outlining how independent assessments of agency efforts to improve and report on their financial management practices, and comply with the Financial Statement Auditability Plan, will be conducted. The simple step of independent verification, which should be conducted by the appropriate IG or by an independent public accountant, will alleviate the current creditability problems regarding the content of an agency's Annual Financial Reports. Further, in order to ensure greater transparency, the Committee requests that all audit opinions concerning elements of the IC be posted annually on the DNI's unclassified Web site. The Web site should have a menu that lists all of the elements of the IC, whether they are evaluated as stand-alone agencies or as part of a larger agency or department, and a corresponding rating of "unqualified," "qualified," "adverse," "disclaimer," or "not conducting an audit."

Finally, the Committee believes that both the Congress and the DNI would benefit from the creation of a consolidated NIP financial statement. Such a statement would provide valuable macro-level data and, once established, offer insight into financial trends within the IC. Therefore, the Committee requests that the DNI begin preparing a consolidated financial statement for the NIP beginning with fiscal year 2010. In accordance with the DNI's Financial Statement Auditability Plan, this statement should be based on the fully auditable data provided by each of the IC agencies by fiscal year 2012. As such, a separate audit will not be required for the consolidated statement.

Chief Financial Officer for the Intelligence Community

It is widely recognized that the IC's process for generating requirements for major acquisitions is broken. For instance, about 70 percent of current major acquisition programs currently have no formally validated requirements. Moreover, the requirements process, like the Intelligence Collection Architecture, is inadequately linked to realistic, long-term budgetary constraints. This has been confirmed by ODNI commissioned studies and in-house analysis. Too often, these "front end" resource allocation activities involve no prioritization, and result in the Chief Financial Officer (CFO) in the ODNI receiving funding requests that do not fit within the available budget and are not accompanied by an associated budget cut to an existing program. One such example is described in the Classified Annex to this report. To remedy this situation, budgetary constraints need to be explicitly considered throughout the entire resource process. In addition, the CFO, whose responsibility it is to prepare a budget for the DNI, needs to be centrally involved throughout the entire decision-making process—not just the budgeting at the end of the process.

By the ODNI's own assessment, the current resource management process is "fragmented, unsynchronized, complex, and opaque." A prominent feature of the DNI's 500 Day Plan is to ad-

dress this problem by devising an end-to-end process to synchronize strategic planning, requirements generation, architecture work, programming, budgeting, and performance management. The Committee has received briefings from the ODNI that make clear this project, referred to as the "Strategic Enterprise Management" (SEM) initiative, is a serious effort, but is not close to achieving its objective. Indeed, it appears that the SEM initiative will not be fully operational until the fiscal year 2011 budget, should the effort survive in the next administration.

The Committee applauds the DNI for undertaking the SEM initiative, but believes that it requires concerted attention by ODNI leadership. Even with that attention, unless one senior officer is exclusively in charge of end-to-end resource management, resource decisions will continue to be slow, needlessly complex, subject to contentious revisits, and certainly not integrated. Further, the Committee believes that the DNI's most potent authority—budgetary control—is not adequately reflected in the ODNI's organizational structure. Accordingly, for the SEM initiative and budgetary control to be effectively executed, the ODNI's organizational structure warrants change.

Therefore, Section 408 of the bill creates the position of the Chief Financial Officer of the Intelligence Community (IC CFO), investing that position with the duties, responsibilities, and authorities of the CFO Act of 1990, as appropriate. The section makes clear that the IC CFO will serve as the principal advisor to the DNI on IC budgetary resources, and that this officer will establish and oversee a comprehensive and integrated strategic process for managing IC resources. Other senior officers may be primarily responsible for certain aspects of this overall process, such as strategic planning or acquisition milestone decision authority, but Section 408 makes the IC CFO responsible for the over-all operation and coordination of all resource processes. The Committee intends and expects that, as the principal advisor to the DNI on resource allocation, the IC CFO will consider and balance the equities of all IC parties in his or her recommendations to the DNI and PDDNI, and that they, in turn, will receive recommendations directly from the IC CFO.

Independent Cost Estimation

The more of the budget that is subjected to the discipline of an Independent Cost Estimate (ICE) or other independent cost assessment, the more realistic and sustainable it will be. Therefore, the bill, by changing the definition of "major system" in provisions of the National Security Act of 1947 related to major system acquisitions (e.g., Section 316) reduces the cost threshold for when a program requires an ICE, and when it must be budgeted to an ICE, from $500 million to about $170 million.

This threshold is used throughout the U.S. government to define a major system acquisition, and its adoption in the bill responds to the ODNI's request to make this definition uniform in statute. The Committee anticipates that the ODNI's Intelligence Community Cost Analysis and Improvement Group (IC CAIG) will delegate many of the resulting additional ICEs for smaller programs to those executing agencies with independent cost estimating capabilities. The Committee also strongly encourages the IC CAIG to con-

tinue to expand its purview to large programs that are not usually considered "systems acquisition," such as IC data centers, the pending cyber initiative, and large personnel increases that function together to fulfill a mission need.

Since these increased IC CAIG duties will require additional personnel, some with a new and different skill set than current professional cost estimators, the classified annex of the bill provides additional personnel without increasing the ODNI total.

Also, while the Committee is impressed with the professionalism and productivity of the IC CAIG, it believes it is incumbent on the IC CAIG to establish and publish the track record of its ICEs in predicting actual program costs. This is especially important given how critical these ICEs have become in guaranteeing budget reality.

Accordingly, the Committee requests the ODNI to include in each President's Budget, or in each annual Program Management Report, a comparison of all IC CAIG ICEs to the actual costs of completed and on-going programs. The comparison will be on a basis that is consistent from year to year and from program to program, and which is a good measure of cost estimating fidelity. Such a comparison may account for changes in program scope, but it must also compare estimates to actual costs without scope changes. The Committee recommends that the IC CFO consult with the Committee on its proposed methodology for establishing such a track record prior to its publication in the President's Budget.

Additionally, to guarantee both continued objectivity and seamless linkage to the budget process, the Committee believes that the ODNI CAIG should continue to report to the ODNI CFO and should not be realigned to any other part of the organization without prior written notification of the Intelligence Committees. Therefore, should the DNI contemplate moving the CAIG outside the office of the CFO, he should notify the Committee no later than 60 days prior to the contemplated move.

Finally, the Committee understands that the Office of the Chief Financial Officer of the CIA has added personnel to conduct cost estimates for CIA programs and projects, but that the process for conducting cost estimates remains ad hoc. There is not a threshold amount above which a cost estimate is required or a requirement that cost estimates occur before a project is underway.

The Committee requests that the Associate Deputy Director of the CIA establish clear guidelines for the conduct of cost estimates for agency acquisitions. This guidance should include the requirement that the CFO conduct a cost estimate for any construction or acquisition project likely to exceed $15 million.

Performance Based Budgeting: Accounting and accountability for results

The DNI seeks to instill in the IC "an execution culture", meaning that carrying through on intention is what really counts and performance is "Job Number One". The Committee applauds this overdue goal. Too often, senior officials appear more concerned with the accretion of dollars and positions than with the performance they are charged to achieve with these resources. Performance-based budgeting is critical to reversing these priorities and bringing about the execution culture the DNI seeks. Performance budg-

eting also holds great promise for making government more transparent and efficient.

The IC's resource management, like that in many parts of the government, is fixated on inputs—the dollars and people it seeks from Congress. Government accounting lays out these inputs in great detail across a myriad of categories. However, there is scant accounting for outcomes. And where accounting does not exist, neither can true accountability. Rarely can the IC express in clear, concrete terms the performance results expected from its requested funding, or the real results from actual expenditures.

Consequently, Congress is routinely asked to authorize and appropriate billions of dollars for programs and activities whose criteria for success or failure the Administration cannot even venture. The presidential directive to increase HUMINT by 50 percent and major elements of the Comprehensive National Cybersecurity Initiative are but two prominent examples in the FY 2009 budget. We have accordingly made significant adjustments to these requests, which are detailed in the Classified Annex.

Performance-based budgets are admittedly difficult. But when done well, they will permit us to know whether, and to what degree, our investments will be judged successful. We will also discover how requested dollars are linked to expected performance. Aside from these accountability and transparency benefits, such linkages permit efficiency measures, which in turn, will enable us to achieve greater efficiency. This is always in the public interest, but it will be imperative if the IC is to accomplish its missions if budgets no longer increase year after year.

Performance Based Budgeting: Major progress made in FY 2009 budget

This year's FY 2009 NIP budget makes great progress towards a performance-based budget. It represents the first rigorous attempt to account for results in a significant portion of the budget. Even so, the DNI and the IC are years behind much of the rest of the government. The FY 2009 budget makes genuine headway in three areas:

- First, it constructs a complete performance-based budget for the DNI's Mission Objective #2—Counter Proliferation. Outcome measures were clear, meaningful, and measurable; baselines and targets appear largely solid; and dollars are explicitly linked to mission performance. This work will serve as the model for constructing a performance budget in the other four Mission Objectives. While some of these mission objectives may change with a new DNI or new administration, the analytical performance model will nonetheless be applicable to any new mission area.
- Second, it lays the foundation for a NIP-wide performance-based budget in the "Budget Categories." These are the seven functional categories based on the intelligence cycle, which are meant to be enduring and should *not* change in a new administration. The Committee judged most measures to be useful, but found measures in the Research and Technology Budget Category to be very weak. Nonetheless, the yearly performance measures for Budget Categories should yield high-level information on the health of intelligence, which should help guide future investment decisions.

- Third, many of the budgets of the NIP components have made progress at the "Expenditure Center" level of detail. This progress should also endure a change of administration, as Expenditure Centers are derived from the Budget Categories. However, the measures in this budget are of highly uneven quality across and within individual NIP components; thus, much work remains.

Performance Based Budgeting: Counterterrorism and other missions lag counter proliferation

For the most part, the performance budget for counter proliferation is a good model for the other Mission Objectives. Owing to the clarity and accountability of Mission Objective 2's performance-based budget, the Committee has favored the administration's request for counter proliferation. We find that the benefit of doubt can shift in favor of the request when we are confident we will be able to make future budgetary adjustments—up or down—based on relevant, measurable performance.

Counterterrorism stands in stark contrast. One of this Mission Objective's two outcome measures is not constructed in a way that lends itself to meaningful targets. There are no baselines, no targets, and no explicit linkage of dollars to results. This is very disappointing, given that counterterrorism is the number one mission priority and that the FBI had already produced a workable performance budget for its counter-terrorism activities.

While the Committee has authorized a robust counterterrorism budget, we remain concerned with fuzzy accounting for results and with uncertain accountability. To further the DNI's efforts to instill a culture of execution in its top mission priority, the Committee has fenced certain funding in the National Counterterrorism Center, pending receipt of a Mission Objective 1 performance budget whose rigor and clarity is comparable to that of Mission Objective 2's.

The performance-based budgets for the DNI's other mission objectives—support democracy, hard target penetration, and early warning—are generally even weaker than for counterterrorism. However, the Committee believes that performance work in these areas should be the lowest priority, as they appear the least likely to endure a change in administration. Also, the Committee urges the DNI to be judicious in keeping all performance measures to a manageable number of key metrics, as each comes with an administrative tail of monitoring, targeting, and reporting. Quality matters here, not quantity.

The Committee expects to receive next year the full performance budget promised by the DNI for FY 2010. It will be prepared to withhold or reduce its authorization levels to the extent this promise is not fulfilled.

Intelligence Community records

The Chief Information Officer of the Intelligence Community is tasked with managing activities relating to the information technology architecture of the Intelligence Community, including the retention and disposal of Intelligence Community records. The Committee is concerned that current policies within the Intelligence Community, as well as current statutory requirements, may not encourage appropriate retention of Intelligence Community

records that would otherwise be useful to the Intelligence Community, the Department of Justice, or the Congress in furtherance of their duties related to elements of the Intelligence Community or its personnel.

The Committee therefore directs that the Chief Information Officer identify specific classes of Intelligence Community records that should be retained for such purposes. The Chief Information Officer shall specify whether current retention or disposal practices are attributable to Intelligence Community policies and procedures or to statutory requirements. The Chief Information Officer shall report such findings to the congressional intelligence committees no later than December 31, 2008.

Compliance with Senate Rule XLIV

The following list of congressionally directed spending items included in the classified annex is submitted in compliance with rule XLIV of the Standing Rules of the Senate, which requires publication of a list of congressionally directed spending items.

A provision adding $200,000 for an Intelligence Training Program run by the Kennedy School of Government. The provision was added at the request of Senator Rockefeller.

A provision adding $2.0 million for biometric research. This provision was added at the request of Senator Rockefeller.

A provision directing $3.5 million to the Naval Oceanographic Command. This provision was added at the request of Senator Wicker.

A provision adding $3.5 million for littoral net centric operations. This provision was added at the request of Senator Rockefeller.

A provision adding $5.5 million for the Space Lab at Utah State University. This provision was added at the request of Senator Hatch.

A provision adding $10.4 million for the National Media Exploitation Center. This provision was added at the request of Senator Rockefeller.

The bill and classified annex contain no limited tax benefits or limited tariff benefits, as defined by Section 103 of S. 1.

COMMITTEE ACTION

Vote to report the committee bill

On May 1, 2008, a quorum for reporting being present, the Committee voted to report the bill subject to amendments, by a vote of 10 ayes and 5 noes. The votes in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—aye; Senator Burr—no.

Votes on amendments to committee bill, this report and the classified annex

On April 29, 2008, by a vote of 9 ayes to 6 noes, the Committee adopted an amendment of Senator Feinstein, Senator Whitehouse, Chairman Rockefeller, Senator Feingold, Senator Wyden, Senator

Hagel, Senator Snowe and Senator Mikulski, (Section 321) to prohibit the use of any treatment or technique of interrogation not authorized by the U.S. Army Field Manual on Human Intelligence Collector Operations on any individual in the custody or under the effective control of personnel of an element of the intelligence community. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—no; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—aye; Senator Burr—no.

On April 29, 2008, by a voice vote, the Committee agreed to an amendment by Senator Burr (an amendment to Section 335) to repeal or modify certain additional reporting requirements.

On April 29, 2008, by a voice vote, the Committee agreed to an amendment by Senator Wyden to authorize an additional amount of funding for information technology within the Federal Bureau of Investigation to ensure desktop access to the Internet as further described in the classified annex to the Schedule of Authorizations.

On April 29, 2008, after agreeing by a voice vote to a second degree amendment by Senator Burr to set a five-year sunset, the Committee agreed by an amendment by Senator Snowe (Section 333) to require the Director of National Intelligence, in coordination with the Director of the Federal Bureau of Investigation, to establish performance metrics and specific timetables related to the FBI carrying out certain matters related to intelligence and national security and to report to the congressional intelligence committees on a semi-annual basis concerning the FBI's progress in improving its performance.

On April 29, 2008, by a voice vote, the Committee agreed to an amendment by Vice Chairman Bond (Section 348) to modify the officials that may be designated to certify that an FBI undercover operation is designed to collect foreign intelligence or counterintelligence.

On April 29, 2008, after agreeing by a vote of 14 ayes to 1 no to a second degree amendment offered by Senator Mikulski, the Committee agreed by voice vote to an amendment by Senator Feingold to direct the DNI to provide certain documents and answers to Committee questions related to privacy and civil liberties, budget assessments, and implementation plans and to prohibit the obligation of certain funds pertaining to elements of the Comprehensive National Cybersecurity Initiative until such documents and answers are received by the congressional intelligence committees. The votes on the second degree amendment in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—no; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—aye; Senator Warner—aye; Senator Hagel—aye; Senator Chambliss—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Burr—aye.

On April 29, 2008, by a voice vote, the Committee agreed to an amendment by Chairman Rockefeller and Vice Chairman Bond (to Section 316) to require certain reports and findings when a major system acquisition is estimated to cause an increase to these future

budget projections and to include certain comments in the report to accompany the bill.

On April 29, 2008, by a vote of 8 ayes to 7 noes, the Committee adopted an amendment of Vice Chairman Bond (Section 345) to limit the reprogramming and transfer of funds if a congressional intelligence committee requests additional information on such activity to a date specified by such congressional intelligence committee up to 90 days after the date of the request. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—no; Senator Feinstein—no; Senator Wyden—no; Senator Bayh—no; Senator Mikulski—no; Senator Feingold—aye; Senator Nelson—no; Senator Whitehouse—no; Vice Chairman Bond—aye; Senator Warner—aye; Senator Hagel—aye; Senator Chambliss—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Burr—aye.

On April 29, 2008, by a voice vote, the Committee agreed to an amendment by Senator Whitehouse, Chairman Rockefeller, Senator Hagel, Senator Feinstein, and Senator Feingold (Section 323) to prohibit the use of funds authorized by the bill to detain any individual under the effective control of an element of the intelligence community if the International Committee of the Red Cross is not provided notification of the detention of and access to the individual.

On April 29, 2008, by a vote of 9 ayes to 6 noes, the Committee adopted an amendment by Senator Feinstein, Chairman Rockefeller, Senator Feingold, and Senator Whitehouse (Section 322) to prohibit the Director of the Central Intelligence Agency from permitting a contractor or subcontractor of the CIA to carry out an interrogation of an individual and to require that all interrogations be carried out by employees. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—no; Senator Burr—no.

On April 29, 2008, by a voice vote, the Committee agreed to an amendment by Senator Whitehouse pertaining to an activity described in the classified annex to the Schedule of Authorizations.

On May 1, 2008, by a vote of 10 ayes to 5 noes, the Committee adopted an amendment by Senator Feingold and Senator Hagel (Title V) to establish the Foreign Intelligence and Information Commission to assess needs and provide recommendations to improve foreign intelligence and information collection, analysis, and reporting. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—aye; Senator Burr—no.

On May 1, 2008, by a voice vote, the Committee adopted an amendment to the classified annex by Senator Chambliss to prohibit the obligation of funds for any covert action finding reported to congressional staff in addition to the staff directors of the con-

gressional intelligence committees until the finding of such program has been briefed to the full membership of the congressional intelligence committees.

On May 1, 2008, by a voice vote, the Committee adopted an amendment by Senator Feinstein and Senator Feingold (Section 331) to require a report from the Director of National Intelligence that describes any activity that is being conducted by one or more contractors that the DNI believes should only be conducted by U.S. government employees, an estimate of the number of the contractors conducting each such activities, and the plan of the DNI, if any, to have each activity conducted by U.S. government employees.

On May 1, 2008, by a vote of 10 ayes to 5 noes, the Committee adopted an amendment by Senator Feinstein and Senator Feingold (Section 332 and Section 344) on (a) notifications to the congressional intelligence committees under Sections 502 and 503 of the National Security Act and (b) the availability of funds under Section 504 of that Act. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—no; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—no; Senator Hatch—no; Senator Snowe—aye; Senator Burr—no.

On May 1, 2008, by a vote of 14 ayes to 1 no, the Committee adopted an amendment by Chairman Rockefeller to the classified annex to include findings of the Committee's HUMINT Review Group. The votes on the amendment in person or by proxy were as follows: Chairman Rockefeller—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Feingold—aye; Senator Nelson—aye; Senator Whitehouse—aye; Vice Chairman Bond—aye; Senator Warner—no; Senator Hagel—aye; Senator Chambliss—aye; Senator Hatch—aye; Senator Snowe—aye; Senator Burr—aye.

On May 1, 2008, by a voice vote, the Committee adopted a substitute amendment by Vice Chairman Bond (to Section 401 which authorizes the DNI to conduct accountability reviews of elements of the Intelligence Community and the personnel of such elements). The substitute amendment additionally requires that the head of an element of the Intelligence Community who makes a determination not to implement a DNI recommendation for corrective or punitive action in relation to a failure or deficiency within the Intelligence Community submit a notice of such determination to the congressional intelligence committees.

On May 1, 2008, by voice vote, the Committee adopted an amendment by Vice Chairman Bond to the report to accompany the bill to include a section on Intelligence Community records.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to this legislation. On May 8, 2008, the Committee transmitted this bill to the Congressional Budget Office and requested

it to conduct an estimate of the costs incurred in carrying out its provisions.

EVALUATION OF REGULATORY IMPACT

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

CHANGES IN EXISTING LAWS

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

ADDITIONAL VIEWS OF SENATORS FEINGOLD AND HAGEL

During consideration of the Fiscal Year 2009 Intelligence Authorization bill, the Committee supported an amendment we offered to establish an independent commission to examine how the United States government gathers information it needs to defend our national security and further our foreign policy goals. The commission will address long-standing impediments to effective overseas collection and strategic analysis. First, as the Director of National Intelligence has testified, the Intelligence Community devotes "disproportionate" resources toward current crises, rather than strategic challenges and emerging threats. Second, the Intelligence Community has not established the "global reach" needed to anticipate those over-the-horizon threats. And, third, the government lacks interagency collection strategies that include not only the Intelligence Community, but also non-clandestine information gathering, particularly by the Department of State. As the Acting Director of the National Counterterrorism Center has testified, diplomatic reporting is "absolutely critical" for understanding conditions that can result in the emergence of new terrorist safe havens and can at times be more effective in obtaining information related to that threat than the Intelligence Community.

To fully and effectively utilize all the collection tools at its disposal, the United States government must develop an interagency strategy that considers first what information it needs, not only currently but in the future, and second who is best positioned to obtain that information. It must then translate that strategy into resource allocations, reflected in budget requests and in the mix of personnel at the country mission level. The commission will consider impediments to an effective, coordinated interagency collection strategy and make recommendations to the Congress and the executive branch.

The Director of National Intelligence has discussed the necessity for at least some analysts to be focused on the unknown threats over the horizon—not just the threats we face today. The commission will also review how well positioned our analytical capabilities are to focus not only on current threats but also on future or emerging threats, in order to avoid strategic surprise.

The commission's mandate extends beyond the Intelligence Community, covering the State Department and other departments and agencies whose reporting contributes to the government's overall understanding of international affairs, as well as the interagency budgetary process. That mandate is thus broader than the authorities of the Director of National Intelligence as well as the jurisdiction of the Committee or any other congressional committee. We anticipate, however, that the recommendations of the commission will prove extremely beneficial to effective congressional oversight of the Intelligence Community, and will contribute to a broader

United States government effort to understand the world and defend our national security interests.

We are pleased that the commission has been supported by prominent foreign policy and intelligence experts, including Zbigniew Brzezinski, Donald Gregg, Larry Wilkerson, Carl Ford, Gayle Smith, David Kay, and Rand Beers.

RUSSELL D. FEINGOLD.
CHUCK HAGEL.

ADDITIONAL VIEWS OF SENATOR FEINGOLD

In addition to an amendment I offered with Senator Hagel to establish an independent commission to review intelligence and foreign information collection, the Fiscal Year 2009 Intelligence Authorization bill and the accompanying classified annex include numerous important provisions.

Foremost is the Committee's bi-partisan approval of an amendment I co-sponsored that would end all interrogations not in compliance with the Army Field Manual. It has long been my position that the CIA interrogation program is morally and legally untenable and is not making our country any safer. Congress's effort to end this Administration's use of "enhanced interrogation techniques" as part of the Fiscal Year 2008 authorization bill was historic. Notwithstanding the veto of that legislation, the Committee is right to continue to insist on interrogation policies that are consistent with our principles as well as with our national security. I was also pleased to co-sponsor an amendment prohibiting CIA contractors from carrying out interrogations.

The bill includes another important amendment I co-sponsored requiring notification of and access by the ICRC to all detainees. At a time when there is global anger against our country because of this administration's indifference to international law, this amendment is not only humane and just, but will help mitigate the damage that the secret CIA detention program has done to our national security.

I was also extremely pleased that the Committee approved an amendment I co-sponsored again this year requiring that all members of the Committee be given some information about intelligence programs that have been limited to the "Gang of Eight." From the President's warrantless wiretapping program to the CIA detention and interrogation program, members of the Committee have been denied access to information they need to conduct effective oversight. This amendment will help bring those abuses to an end.

Many other provisions of the bill provide important support for our nation's intelligence activities, while promoting reform and accountability. Among them is an amendment I offered limiting funding for elements of the Comprehensive National Cybersecurity Initiative pending receipt of documents and answers to Committee questions related to privacy and civil liberties, budget assessments, and implementation plans.

RUSSELL D. FEINGOLD.

ADDITIONAL VIEWS OF SENATOR WHITEHOUSE

If we go down the corridors of history and survey the evil practices of tyrant regimes, we would find that one of their most notorious methods of coercion and subjugation is holding prisoners incommunicado. This Committee has sought to address this issue in this intelligence authorization bill.

Specifically, the Committee passed by voice vote an amendment that I offered, cosponsored by Chairman Rockefeller and Senators Hagel, Feinstein, and Feingold, that would require that detainees held by any element of the United States Intelligence Community be made available to the International Committee of the Red Cross (ICRC) on the same terms on which they are required to be made available when they are held by the United States military. These terms recognize the secure confidentiality respected by the ICRC, and allow necessary flexibility based on military necessity.

This provision is consistent with and central to the fundamental premise of international law that no one should be detained beyond the bounds of the law. A seminal text on this subject, "The Treatment of Prisoners under International Law," describes "the prohibition of incommunicado detention" as among "the most central" of all recognized international detainee safeguards.

This safeguard has long been honored and advocated by the United States military, which has recognized that the ICRC is "presumptively authorized [to have] access to detainees." The U.S. military notes this access "is based on the special role established by international law for the ICRC to monitor compliance with the law of war." When U.S. armed forces personnel have been detained, the United States has argued for prompt access. President George W. Bush reacted when our Navy patrol aircraft was forced to land in China after a mid-air collision by saying that, "[t]he first step should be immediate access by our embassy personnel to our crew members." He continued, "I call on the Chinese government to grant this access promptly." The United States has been a strong advocate opposing "disappearances" on a worldwide basis. U.S. law has long prohibited assistance to any government which engages in a consistent pattern of gross violations of internationally-recognized human rights, including "prolonged detention without charges, causing the disappearance of persons by the abduction and clandestine detention of those persons[.]" Just last month, the U.S. Department of State, in its annual human rights report, criticized the governments of North Korea, Burma and Sri Lanka for engaging in "disappearances."

Moreover, prohibiting incommunicado detention has been a bipartisan endeavor. In 2005, Senator John McCain advocated a requirement for ICRC access across the board for all military detainees in Senate Amendment No. 1557, cosponsored by Senator John Warner, among others, to S. 1042, the National Defense Authoriza-

tion Act of Fiscal Year 2006. As Senator McCain said in 2004: "We distinguish ourselves from our enemies by our treatment of our enemies.

Were we to abandon the principles of wartime conduct to which we have freely committed ourselves, we would lose the moral standing that has made America unique in the world."

The tradition and moral authority of this goes all the way back to the Gospel according to Matthew, Chapter 25, verses 36–40. "I was naked and you clothed me. I was sick and you visited me. I was in prison and you came to me." This applies even to those who are, to quote Matthew again, "the least of our brethren."

The international standard for detention of detainees in armed conflicts is the access of the International Committee of the Red Cross. It is simply a matter of human decency, and I am gratified that the Committee chose to apply this standard to detentions by the U.S. intelligence community, just as it applies to the military.

SHELDON WHITEHOUSE.

ADDITIONAL VIEWS OF SENATOR SNOWE

After successfully passing an Intelligence Authorization Bill for twenty-seven consecutive years, it is unconscionable that Congress has failed to pass a bill for the past three. At a time when our nation is bogged down in Iraq, a National Intelligence Estimate has concluded that Al Qaeda is driven by an undiminished intent to attack the Homeland and has regenerated key elements of its homeland attack capability, and costly intelligence programs have been marked by overruns, it is time that the Congress reassert itself as the constitutional check to the Executive Branch and pass an intelligence authorization bill to provide policy guidance and set funding levels for the entire intelligence community. This bill is undoubtedly a step toward greater transparency and accountability that is long overdue.

Importantly, this bill includes a provision that would create an inspector general of the entire intelligence community. The inspector general provision is based upon a bill that I introduced in 2004. I believe that one key way to prevent the same mistakes from happening again is to inject more accountability into the Intelligence Community, and it is my hope that by creating a sound, strong, and aptly-equipped Inspector General, we will achieve this goal.

The language pertaining to the inspector general provision has broad bi-partisan support. There are indeed some contentious provisions in the Intelligence Authorization bill—but this is not one of them. Amazingly, our Intelligence Community still does not have an independent Senate-confirmed inspector general who can initiate and conduct investigations of elements within its ranks, despite the systemic failures of both 9/11 and Iraq WMD. According to the Inspector General Act of 1978, an inspector general looks independently at problems and possible solutions, yet the current construct of the Office of Inspector General of the Office of the Director of National Intelligence does not allow the Inspector General to investigate the various elements within the Intelligence Community. How can an Inspector General be expected to do his or her job without the right to investigate the various elements?

As a member of the Intelligence Committee, I have been at the vanguard of countless investigations, reports and debates on intelligence community practices. Too many incidents of failure to prevent attacks, to properly collect the necessary intelligence, to adequately analyze that intelligence, and to share information within the community beg for better accountability in the entirety of the community. An Inspector General of the intelligence community who can look across the intelligence landscape will help improve management, coordination, cooperation, and information sharing among the agencies—the current construct does not get the job done! The Inspector General of the Intelligence Community, which is included in this bill, will have subpoena power and the ability

to investigate current issues within the Intelligence Community—to identify problem areas and find the most efficient and effective business practices required to ensure that critical deficiencies can be addressed before it is too late—before we have another intelligence failure.

We must ensure that an Inspector General, with community-wide powers and a mandate to bring accountability, is part and parcel of the future if we are to establish an intelligence apparatus equal to the new challenges of 21st century threats.

Significantly, the bill also includes a provision that I introduced and which was passed by a voice vote that would accelerate the intelligence transformation at the FBI, as the FBI has yet to make the dramatic changes necessary to address the threats facing our nation. The amendment would require the Director of National Intelligence (DNI) to coordinate with the FBI to establish performance metrics and specific timetables and submit to Congress a semi-annual report evaluating the timetables, corrective actions, and activities necessary to ensure the FBI is improving its performance.

In December 2005, the 9/11 Commissioners offered their final report on intelligence reform and gave the FBI a "C". The report stated:

> Progress is being made—but it is too slow. The FBI's shift to a counterterrorism posture is far from institutionalized, and significant deficiencies remain. Reforms are at risk from inertia and complacency; they must be accelerated, or they will fail. Unless there is improvement in a reasonable period of time, Congress will have to look at alternatives.

The Commission also concluded that "the Bureau ha[d] announced its willingness to reform and restructure itself to address transnational security threats, but has fallen short—failing to effect the necessary institutional and cultural changes organizationwide." A subsequent press report also noted that the "FBI culture still respects door-kicking investigators more than deskbound analysts sifting through tidbits of data" and that "the uneasy transition . . . has prompted criticism from those who believe that the bureau cannot competently gather domestic intelligence." In August of 2006, Governor Kean, the Chairmen of the 9/11 Commission, stated that the FBI had moved too slowly to improve its ability to prevent future terrorist plots, was plagued by turnover in its senior ranks, and was "not even close to where they said they would be." Then an April 2007 DOJ Inspector General report found that the professional divide between analysts and special agents remains a problem, and that the barriers to acceptance and cooperation between the two groups must be addressed if the FBI is to efficiently and effectively meet its mission of preventing terrorist acts.

This Committee concluded that "nearly seven years after the attacks of September, 11, 2001, the FBI has yet to make the dramatic leaps necessary to address the threats facing our nation." Our nation is facing a persistent and preeminent threat from violent extremism and there must be a sense of urgency in addressing that threat. As the committee charged with legislative oversight

over the intelligence activities of the United States, it is imperative that the Intelligence Committee begin to mandate the pace of reform at the Bureau. I asked Governor Kean during the October 2007 FBI transformation hearing what the Committee could do to elevate certain intelligence functions at the Bureau, and Governor Kean told the committee that "I think that under the leadership of this Committee, you have to make it very clear that what's going on up to this point is unacceptable . . . and perhaps you should establish goals . . . mandates . . . you say 'we expect this to be done' as a Committee." This bill directs the DNI to submit to the congressional intelligence committees a consolidated report on the progress of the FBI, including an assessment of the metrics, timetables and corrective actions, and a description of the activities being carried out to ensure the Bureau is improving its performance. We can no longer afford to give such deference to the FBI regarding its intelligence reform. The threat is too urgent for us to not intervene.

OLYMPIA J. SNOWE.

MINORITY VIEWS OF VICE CHAIRMAN BOND AND SENATORS WARNER, CHAMBLISS, HATCH, AND BURR

After three straight years without an intelligence authorization law, we hoped that 2008 would be the year to re-establish legislative oversight. We hoped that Members of the Senate Intelligence Committee would finally put aside political interests and focus on national security by voting out a clean bill that could pass the House and Senate and be signed by the President. We hoped that Members would see the detriment, to both the credibility of the Committee and to the Intelligence Community we oversee, of four straight years without an intelligence authorization law. Unfortunately, once again, it seems that politics won out over credibility, oversight, and national security.

A majority of Committee members voted again to include a provision in this year's bill that was responsible for drawing a Presidential veto on last year's bill. They voted to send a political message to critics of the CIA's interrogation program, at home and abroad, at the expense of four years of accumulating, necessary legislation and sound oversight. In fact, they voted to send this message at the expense of reforming the very program they say they want to change, because all of the provisions in the bill which actually do reform the CIA's interrogation program will now likely never become law. This is unfortunate because there is a lot of room for agreement in this area and there is certainly room for agreement in finding a way to do what the supporters of this amendment say they want to do—prohibit harsh interrogation techniques.

The media often report that the Army Field Manual (AFM) amendment does exactly that—prohibits harsh interrogation techniques—but that is not what the amendment says. Rather, it stipulates that all U.S. government interrogators be limited to using only the 19 techniques that are specifically authorized in the AFM. The problems with this limitation are three-fold.

First, as the Director of the Central Intelligence Agency General Hayden has said repeatedly, "I don't know of anyone who has looked at the Army Field Manual who could make the claim that what's contained in there exhausts the universe of lawful interrogation techniques consistent with the Geneva Convention." In other words, if there are interrogation techniques available that are legally and morally permissible under all other U.S. laws and treaty obligations—and we believe there are—why would we want to prevent our interrogators from using these techniques to obtain information that may save American lives? Additionally, innovative interrogators in the future may develop new techniques that are also legally and morally permissible that were not developed at the time the AFM was drafted. At a time when we are fighting a global war

on terrorism, it makes no sense to remove legally and morally acceptable tools from the hands of our intelligence operatives.

Second, this restriction may have unintended consequences that have not been fully examined. Before we legislate that *all* government agencies must use *only* the techniques in the AFM, we must make sure that these agencies can use *any and all* other moral and legal techniques. For example, currently the Federal Bureau of Investigation is permitted to use deception in an interrogation about the evidence against a detainee. The AFM is unclear about the extent to which such deception could be used in an interrogation setting. Would the FBI, therefore, be prohibited from using this technique? What spillover effects would such a prohibition have in the FBI's criminal work? These are serious potential consequences that need to be explored.

Third, the list of the 19 permitted interrogation techniques are published in an unclassified document that is widely available on the Internet. We know that al-Qa'ida terrorists are using the AFM as a training document and are preparing themselves to resist questioning from our interrogators. We should not allow the full complement of our interrogation techniques to be disclosed to the world's most hardened terrorists.

The AFM amendment has other problems as well. Most significantly, because the AFM can be changed at the discretion of the Secretary of the Army—and presumably at the direction of the Secretary of Defense, the President, and perhaps others—the AFM amendment would essentially delegate lawmaking to a service secretary or other members of the Executive branch. Such an abdication of Congressional responsibility should give all Members pause.

Finally, the AFM is a military document with specific chain-of-command authorization requirements for use of certain techniques. These requirements are not easily transferable to the CIA or the FBI and would cause uncertainty for our interrogators.

A RESPONSIBLE ALTERNATIVE

Rather than limit our interrogators to a specific number of unclassified interrogation techniques they *can* use, we believe a better alternative would be a proposal raised by Vice Chairman Bond at the Committee's mark-up which would prohibit the use of those techniques that are banned in the AFM. This alternative would provide a strong bipartisan option for Congress to prohibit the use of harsh interrogation techniques and make a statement to those at home and abroad about our values, while preserving the flexibility of our interrogators to use those techniques that are lawful, moral, and comply with Common Article 3 of the Geneva Conventions in the defense of the nation's security.

If proponents of the AFM amendment really want to prohibit "torture" as they claim, they could support a provision that would codify such prohibitions in statute, rather than impose an unclassified military manual on Intelligence Community interrogators that would foreclose the possibility of developing new lawful interrogation techniques to use against terrorists. An Intelligence Authorization bill that contains a simple prohibition against the use of specific harsh interrogation techniques, rather than the AFM provision, would actually have a chance of becoming law. We're not sure

why the Committee chose to give the Administration another blank check in national security oversight, for the fourth time, by insisting upon a provision which they know will doom the bill. We would rather establish that oversight, effectively.

CHRISTOPHER "KIT" BOND.
JOHN WARNER.
SAXBY CHAMBLISS.
ORRIN G. HATCH.
RICHARD BURR.

○