Calendar No. 499

108TH CONGRESS
2d Session

SENATE

REPORT
108–258

TO AUTHORIZE APPROPRIATIONS FOR FISCAL YEAR 2005 FOR INTELLIGENCE AND INTELLIGENCE-RELATED ACTIVITIES OF THE UNITED STATES GOVERNMENT, THE INTELLIGENCE COMMUNITY MANAGEMENT ACCOUNT, AND THE CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM, AND FOR OTHER PURPOSES

MAY 5, 2004.—Ordered to be printed

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

R E P O R T

[To accompany S. 2386]

The Select Committee on Intelligence (SSCI or Committee), having considered the original bill (S. 2386), to authorize appropriations for fiscal year 2005 for intelligence and intelligence-related activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes reports an original bill without amendment favorably thereon and recommends that the bill do pass.

CLASSIFIED SUPPLEMENT TO THE COMMITTEE REPORT

The classified nature of United States intelligence activities precludes disclosure by the Committee of details of its budgetary recommendations in this Report. The Committee has prepared a classified supplement to this Report which contains (a) the Classified Annex to this Report and (b) the classified Schedule of Authorizations which is incorporated by reference in the Act and has the same legal status as public law. The Classified Annex to this Report explains the full scope and intent of the Committee's action as set forth in the classified Schedule of Authorizations. Reports required by the Classified Annex and this Report have been incorporated by reference in Section 105 of the Bill. In addition, the Committee expects the Intelligence Community to comply with any other directions as requirements contained therein as it would any other statutory requirement.

The classified supplement to the Committee Report is available for review by any Member of the Senate, subject to the provisions of Senate Resolution 400 of the 94th Congress.

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

SECTION-BY-SECTION ANALYSIS

The following is a section-by-section summary of the fiscal year 2005 Intelligence Authorization Act. Following the section-by-section analysis there are general Committee comments on other matters.

TITLE I—INTELLIGENCE ACTIVITIES

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 2005.

Section 102 makes clear that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities and applicable personnel ceilings covered under this title for fiscal year 2005 are contained in a classified Schedule of Authorizations. The Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103 authorizes the Director of Central Intelligence (DCI), with the approval of the Director of the Office of Management and Budget (OMB), in fiscal year 2005 to authorize employment of civilian personnel in excess of the personnel ceilings applicable to the components of the Intelligence Community under section 102 by an amount not to exceed two percent of the total of the ceilings applicable under section 102. The DCI may exercise this authority only if necessary to the performance of important intelligence functions. Any exercise of this authority must be reported to the intelligence committees of the Congress.

Section 104 authorizes appropriations for the Intelligence Community Management Account (CMA) of the DCI and sets the personnel end-strength for the Intelligence Community Management Staff for fiscal year 2005.

Subsection (a) authorizes appropriations of $342,995,000 for fiscal year 2005 for the activities of the CMA of the DCI. Subsection (a) also authorizes funds identified for advanced research and development to remain available for 2 years.

Subsection (b) authorizes 310 full-time personnel for elements within the CMA for fiscal year 2005 and provides that such personnel may be permanent employees of the CMA element or detailed from other elements of the United States Government.

Subsection (c) authorizes additional appropriations and personnel for the CMA as specified in the classified Schedule of Authorizations and permits the additional funding amount to remain available through September 30, 2006.

Subsection (d) requires that, except as provided in section 113 of the National Security Act of 1947, personnel from another element of the United States Government shall be detailed to an element of the CMA on a reimbursable basis, except that for temporary functions such personnel may be detailed on a non-reimbursable basis for periods of less than 1 year.

Subsection (e) authorizes $34,911,000 of the amount authorized in subsection (a) to be made available for the National Drug Intelligence Center (NDIC). Subsection (e) requires the DCI to transfer these funds to the Department of Justice to be used for NDIC activities under the authority of the Attorney General, and subject to section 103(d)(1) of the National Security Act.

Section 105 incorporates into the Act by reference each requirement to submit a report contained in the joint explanatory statement to accompany the conference report or in the associated classified annex to the conference report.

Section 106 authorizes, solely for the purposes of reprogramming under Section 504(a)(3) of the National Security Act of 1947 (50 U.S.C. 414(a)(3)), those funds appropriated for an intelligence or intelligence-related activity in fiscal year 2004 in excess of the amount specified for such activity in the classified Schedule of Authorizations that accompanied H.R. 2417, the Intelligence Authorization Act for Fiscal Year 2004 (H.R. Report 108–381).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

AUTHORIZATION OF APPROPRIATIONS

Section 201 authorizes appropriations in the amount of $239,400,000 for fiscal year 2005 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL PROVISIONS

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

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

Section 303 amends the National Security Act of 1947 by removing the ''unforeseen requirements'' criterion from section 504(a)(3) of the Act (50 U.S.C. 414(a)(3)) (relating to the funding of certain intelligence activities by reprogramming). The amendment ensures that the Intelligence Community, in cooperation with the Committees, can react more quickly to confront higher-priority needs, by eliminating unnecessary and time-consuming legal debates with respect to proposed reprogrammings. Elimination of the unforeseen requirements criterion will permit reprogrammings to be reviewed on the basis of relative needs and priorities.

Section 304 amends the Foreign Intelligence Surveillance Act (FISA) of 1978 by expanding the definition of an ''agent of a foreign power'' to include ''any person, other than a United States person,

who * * * engages in international terrorism or activities in preparation therefor.'' This provision is identical to Section 1 of S. 113 as passed by the Senate on May 8, 2003.

Since FISA's enactment in 1978, the targets of intelligence collection and their means of communication have changed dramatically. Intelligence Community collection efforts are increasingly challenged by enhancements in communications technology and by the changing nature of intelligence targets. This provision permits the Government to apply for a FISA warrant to monitor a foreign person—i.e., not a citizen or lawful permanent resident of the United States—engaged in or preparing to commit terrorist activities, even if it is not known whether the foreign person is connected to a group engaged in or preparing to commit similar activities. If the Foreign Intelligence Surveillance Court grants a FISA order, the Government will be able to monitor the activities of the foreign person via electronic surveillance or physical searches, as authorized by FISA. This amendment takes better account of current operational realities without damaging important privacy interests of U.S. persons.

Finally, this section also contains a sunset provision tied to the existing sunset provision in section 224 of the USA PATRIOT Act of 2001 (Public Law 107–56; 115 Stat. 295).

Section 305 contains an additional FISA reporting requirement. This section is identical to Section 2 of S. 113, as passed by the Senate on May 8, 2003.

Section 306(a) repeals the eight-year limit on continuous service on the Select Committee on Intelligence. The limit was included nearly 30 years ago in Senate Resolution 400 (1976) which established the Committee. The need for sustained oversight of the Intelligence Community, including over difficult technical and budgetary issues, has persuaded many informed observers that term limits arbitrarily deprive the Senate of the experience gained from extended service on the Committee.

Section 306(b) makes clear that this amendment is an exercise of the rulemaking power of the Senate, and that it is within the constitutional right of the Senate to make any future change in the Resolution by action of the Senate alone in a simple resolution or in such other measure as the Senate may select.

TITLE IV—CENTRAL INTELLIGENCE AGENCY

Section 401 amends the Central Intelligence Agency (CIA) Voluntary Separation Pay Act (VSPA) by repealing the otherwise applicable September 30, 2005 termination date for CIA's authority under that statute and by eliminating the 15 percent fee previously required to be paid by the CIA pursuant to section 2(i) of the VSPA. The CIA has used its Voluntary Separation Incentive Program (VSIP) authority over the past five years to restructure its workforce to support the DCI's Strategic Direction. The changes in the workforce required to support the DCI's direction affect a number of areas within the Agency. Authority to offer incentives to targeted groups of employees to encourage separation from employment, therefore, remains important to the success of the Agency's restructuring. Security considerations also support vesting the CIA with permanent authority to administer a CIA-specific VSIP for all CIA officers and employees, whether in the Central Intelligence

Agency Retirement and Disability System, the Civil Service Retirement System, or the Federal Employee Retirement System. Section 401 also amends the Federal Workforce Restructuring Act (FWRA) of 1994 by deleting payments made under VSPA from the definition of voluntary separation incentive payments in the FWRA.

Section 402 amends the Central Intelligence Agency Act of 1949 by adding a new section that enhances the cover of certain CIA employees. This new section provides that, notwithstanding any other provisions of law, the DCI, in order to protect intelligence operations and sources and methods, may: pay salaries, allowances, retirement, insurance, and other benefits to CIA employees under non-official cover in a manner consistent with their cover; exempt a category of CIA employees from certain U.S. Government rules and regulations; allow certain CIA employees to claim and receive the same Federal and state tax treatment available to individuals in the private sector; and, allow certain CIA employees to receive Social Security benefits based on the Social Security contributions made.

TITLE V—DEPARTMENT OF DEFENSE INTELLIGENCE ACTIVITIES

Section 501 removes the sunset provision associated with Department of Defense authority to conduct commercial activities necessary to provide security for intelligence collection activities abroad. This authority was first granted in 1991 (Public Law 102–88, Sec. 504) with a sunset date of December 31, 1995. Since enactment in the Intelligence Authorization Act for Fiscal Year 1991, the authority has been extended on four occasions (Public Law 104–93, Public Law 105–272, Public Law 106–398, and Public Law 107–314). Given these four previous extensions and the importance of the authority to Department of Defense intelligence activities, this provision permanently extends the authority and the associated requirements for the conduct of these activities.

Section 502 provides a necessary Defense intelligence exemption to a provision of the Privacy Act (5 U.S.C. 552a). Section 552a(e)(3) of Title 5, United States Code, requires each agency that maintains a system of records to inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual, of:

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

To improve the ability of intelligence personnel of the Department of Defense to recruit sources, it is necessary for Defense intelligence personnel, without having to divulge their affiliation with the Department or the U.S. Government, to approach potential

sources and collect personal information from them to determine their suitability and willingness to become intelligence sources.

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

Section 503 of the Intelligence Authorization Act for Fiscal Year 1995 (Public Law 103–359) granted Defense intelligence personnel a very limited exemption from Section 552a(e)(3), i.e., the exemption is limited to a single ''initial assessment contact outside the United States.'' Current counterterrorism operations highlight the need for greater latitude for assessing potential intelligence sources, both overseas and within the United States. Amending the Privacy Act to give Defense intelligence officers the same protection enjoyed by CIA when assessing and recruiting sources should serve to protect these officers and shield their operations. This should improve the Defense Department's ability to conduct successful human intelligence operations.

Section 503 allows funds available for intelligence and intelligence-related activities to be used to support a unified campaign against drug traffickers and terrorist organizations in Colombia. It is identical to section 502 of Public Law 108–177, the Intelligence Authorization Act for Fiscal Year 2004.

COMMITTEE COMMENTS

A. Intelligence Community Reform

The Committee's examination of our government's handling of the events leading to the September 11th attacks and the Intelligence Community's prewar assessments concerning Iraq's weapons of mass destruction programs have and will highlight a number of problems with our intelligence processes. The findings of the National Commission on Terrorist Attacks Upon the United States (''the 9/11 Commission'') have only added to a growing concern that changes must be made to address these problems. Although Congress and the President have acknowledged publicly the need for Intelligence Community reform, there is not yet a consensus on when and how to enact such reform.

There will likely never be an ideal time for Intelligence Community reform. Change is always difficult, especially in the middle of a war. The threats our nation faces, however, show no signs of abating. While we have made much progress, in some areas the threat appears to be increasing. Therefore, the Committee believes that the process of reform must begin.

The Committee will undertake a deliberate and comprehensive review of the full range of options for modernizing the Intelligence Community. Individual committee members have identified specific areas for reform including organizational structure, accountability, alternative analysis, security clearance procedures, and others.

Other members of Congress have offered reform proposals, as well. We strongly believe that all options are on the table.

As the Committee embarks on this process, we will be guided by an important principle: first, do no harm. Congress must resist the impulse to make quick, politically expedient changes. Our actions should address identifiable problems and ensure that change is institutionalized as a continuous process in the Intelligence Community. The Committee must leave in place a system that will continue to adapt to new priorities and threats without waiting for yet another act of Congress.

The Committee intends to hold a number of hearings focusing specifically on the findings of the Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, the 9/11 Commission, and the initial report of this Committee on the Intelligence Community's prewar assessments concerning Iraq's weapons of mass destruction. In addition, the Committee will hold open hearings in the coming weeks to consider the relative merits of a variety of reform proposals.

The Committee will also be informed by other studies and reports on intelligence activities of the United States prepared over the past two decades. As we consider various courses of action, we intend to work closely with other Committees of jurisdiction and the executive branch. The Committee retains the option of seeking the enactment of reforms during the present session, either in this Act, as it works its way through the legislative process, or in a separate measure.

B. Reporting Requirement—Management of the Intelligence Community as an Information Enterprise

The U.S. Government must fundamentally reexamine the manner in which the Intelligence Community manages intelligence information. In many instances, the intelligence failures that preceded the terrorist attacks of September 11, 2001 were marked by an insistence—whether historically or legally grounded—that intelligence information must be tightly controlled by the intelligence collector. Often, this position was based on a mistaken predicate, namely that an agency "owned" information that it had collected.

In the aftermath of September 11, this Committee, the Joint Inquiry into the Terrorist Attacks of September 11, 2001, the 9/11 Commission, and various commentators have decried the "wall" between Federal Bureau of Investigation criminal and intelligence investigators, the inability of analysts to access crucial operational information on human intelligence sources, the lack of access by intelligence analysts to Foreign Intelligence Surveillance Act and other signals intelligence data, and a lack of commitment to the provision of threat information to State and local officials. In fact, one of the important intelligence reforms in the USA PATRIOT Act (Public Law 107–56) was the dismantling of the "wall" between law enforcement and intelligence. Nevertheless, restrictions on data access by intelligence analysts—some real and some perceived—have been brought to the attention of this Committee on numerous occasions during the course of our continuing oversight of the Intelligence Community.

Although sources and methods must be protected from unauthorized disclosure, the Intelligence Community continues to constrain

its analysts through outdated restrictions on information access and a stubborn refusal to revisit legal interpretations and policy decisions that predate the asymmetric threats that now confront the United States. Given the evolving nature of the challenges confronting the United States, the agencies that comprise the intelligence collection and analysis branches of the U.S. Government must begin using information like a Community—not a loose affiliation of agencies.

The Intelligence Community must be managed as an information enterprise. Pilot programs, ad hoc memoranda of understanding, and "fixes" based on the crisis of the moment are insufficient responses to an endemic problem. Although efforts have been made to surmount restrictions, some information sharing limitations have reemerged in the very programs that were designed to address them. The operations of the Terrorist Threat Integration Center (TTIC) are a prime example of this transfer of limitations. Although TTIC was established to bring intelligence data from across the Intelligence Community together at one location, many analysts at TTIC are still burdened by the same information restrictions that inhibited their work at their parent agency—working under a collage of minimization procedures, parent organization legal authorities and policy barriers, and perceived limitations that still inhibit real all-source intelligence analysis.

This Committee is impatient for real reforms in information sharing and data access. Intelligence data that is collected by the U.S. Government belongs to the U.S. Government—not the intelligence agency that happened to collect it. By making intelligence data available to a Community of all-source intelligence analysts and by providing intelligence information, in classified or unclassified form, to appropriate State and local officials, the United States will be in a better position to address the threat environment confronting the nation. Recognizing the fundamental protections afforded by the Constitution, the nation must reassess legal interpretations, policy directives, and other limitations in statute, Executive order, and regulation that prevent intelligence analysts from accessing the intelligence data they need to complete their important work.

In response to several reporting requirements in the Intelligence Authorization Act for Fiscal Year 2004 (Public Law 108–177), the Intelligence Community Deputies Committee approved the establishment of an "Information Sharing Working Group" (ISWG). Among other things, the ISWG was assigned the task of identifying impediments to information sharing through an analysis of all existing Intelligence Community and Department of Defense policies and laws. As evidenced by Section 354 in the Fiscal Year 2004 Intelligence Authorization Act, Congress has a direct interest in a comprehensive examination of these topics. To that end, the Committee directs the Director of Central Intelligence, to coordinate with the Attorney General and Secretary of Defense, in completing the ISWG review.

The ISWG should include in its review all applicable statutes, Executive orders, regulations, policies, and legal interpretations that inhibit all-source analysis by Intelligence Community analysts. This review should be a zero-based assessment of intelligence collection and analysis authorities and the effect these authorities

and their interpretations have on all-source analysis. The review should include a fundamental analysis of the protections afforded U.S. citizens, lawful permanent residents, and foreign nationals under the Constitution and the impact these protections have on intelligence analysis. It should include a list of all identified inhibitors, as well as an analysis of the statutory, regulatory, legal, or policy bases for such restrictions. Given the difficulties associated with this comprehensive task, the Committee directs that the ISWG report on these issues be provided to the Committee no later than February 1, 2005.

Based on the analysis contained in the ISWG report, the Committee requests that the President inform the Committee of recommendations for overcoming the restrictions outlined in the report. The Committee is particularly interested in recommendations that include a reexamination of existing legal authorities, the creation of an Intelligence Community-wide procedure for minimizing all types of intelligence data to protect the privacy interests of U.S. persons, and the modification of existing agency authorities that restrict all-source analysis, whether in statute, Executive order, regulation, or policy.

C. Intelligence Community Compliance With Federal Financial Accounting Standards

For several years, the Committee has been concerned with the Intelligence Community's financial management practices. In the report accompanying S. 1428 (S. Rpt. 107–63), the Committee instructed the Director of Central Intelligence and the Secretary of Defense to ensure that the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Geospatial Intelligence Agency (NGA), and the Central Intelligence Agency (CIA) receive an audit of their financial statements no later than March 1, 2005, to be performed by a statutory Inspector General or a qualified independent public accountant.

Reports issued by the Department of Defense (DOD) and CIA Inspectors General in 2002 indicated that NSA, DIA, NGA, and CIA were unable to produce auditable financial statements. Unfortunately, this remains the case. In contrast to these agencies, NRO received an unqualified (clean) opinion for its Fiscal Year 2003 financial statements.

The Committee previously acknowledged that NSA, DIA, and NGA may be affected by DOD plans to implement a Department-wide Financial Management Modernization Program, which is not expected to be completed before 2007. The Committee notes that in testimony before a Senate Armed Services subcommittee in March 2004, the Under Secretary of Defense (Comptroller) indicated that DOD plans to earn a clean opinion for its Fiscal Year 2007 financial statements, even though its Modernization Program will not yet be complete.

In recognition of the challenges presented by the difficulties in acquiring the systems necessary to produce financial statements, the Committee indicated in Senate Report 108–44, accompanying S. 1025, the Senate-passed Fiscal Year 2004 Intelligence Authorization Act, that it would consider an extension of the auditable financial statement due date, provided that the relevant agencies offered evidence of significant progress in this area.

Information furnished by the agencies within the last year has revealed numerous positive developments. For example, NGA planned to triple its accounting staff and move to a single accounting system. DIA created a Chief Financial Executive position reporting directly to its Director, and it was rated third among thirty DoD agencies for the quality of its internal controls. NSA received a DoD exemption to purchase financial system software in March 2003 that will assist in modernizing its financial management systems and has developed a detailed implementation plan for the new system. This should allow NSA and, in turn, DIA (which uses portions of the NSA's accounting system) to produce auditable statements by 2007.

Based on this and other information provided by the agencies, the Committee is satisfied that meaningful measures have been devoted to producing auditable financial statements. Substantial obstacles remain, however, and the Committee believes that maintaining the original March 1, 2005, deadline would be counterproductive in that it would require audits that would divert resources from actual financial system improvements.

Accordingly, the Committee has decided that it would not, and does not, object to extending the due date set in the report accompanying S. 1428 (S. Rpt. 107–63), for NSA, DIA, and NIMA/NGA to March 1, 2007, to allow for audits of the Fiscal Year 2006 financial statements. This change does not affect CIA, which is required by Public Law 107–289 to submit audited financial statements for Fiscal Year 2004.

Although obtaining unqualified opinions by March 2007 will be a formidable task, the Committee believes that these efforts are an essential part of bringing further accountability to the Intelligence Community's financial management practices. The need for sound financial management practices has grown in importance with the large amount of supplemental funding received by these agencies in the last several years.

The Committee expects Agency heads to continue to monitor these efforts closely and provide annual progress reports by December 1 of each year preceding the audit requirement.

D. Supplemental Funding of Counterterrorism

The Committee notes a shortfall in Intelligence Community counterterrorism funding in the Administration's Fiscal Year 2005 baseline submission. While the Committee has been advised that additional funding for Intelligence Community counterterrorism activities will be forthcoming in the form of supplemental funds within the Fiscal Year 2005 Defense Appropriations Bill, we are increasingly concerned about the continuing practice of funding known operational requirements through supplemental funding vehicles.

While the practice of funding baseline expenditures using supplemental vehicles has become more prevalent in the past 10 years, the Committee believes that it is time to rein in this practice. The global war on terrorism has been underway for almost 3 years. The Administration and Congress have acknowledged that this conflict will continue for the foreseeable future. The funding requirements for this effort no longer qualify as emergency funding. With respect to the Intelligence Community, these requirements are, and will re-

main for some time to come, day-to-day operational costs of doing business.

Reliance on supplemental funding requests to fund reasonably predictable baseline requirements complicates unnecessarily the execution of new and ongoing operations. The Congress has recently funded supplemental requests and will, more than likely, continue to do so. Nonetheless, operators in the field deserve a greater degree of certainty when it comes to questions of resources—the operators' life-blood. The Committee believes that the global war on terrorism is no longer an emergency funding issue, but rather a long-term reality to which the nation must adapt.

Consequently, the Administration should make a concerted effort to develop reasonable cost estimates for counterterrorism-related intelligence activities over the Future Years Defense Plan or some other acceptable time period. These costs should be included in the future baseline funding requests of the Intelligence Community agencies.

○