108TH CONGRESS
1st Session

SENATE

REPORT
108–44

AUTHORIZING APPROPRIATIONS FOR FISCAL YEAR 2004 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

MAY 8, 2003.—Ordered to be printed

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

R E P O R T

[To accompany S. 1025]

The Select Committee on Intelligence (SSCI or Committee), having considered the original bill (S. 1025), to authorize appropriations for fiscal year 2004 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 pass.

CONTENTS

19–010

CLASSIFIED SUPPLEMENT TO THE COMMITTEE REPORT

The classified nature of United States intelligence activities prevents the Committee from disclosing the 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 the 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 AND EXPLANATION

The following is a section-by-section summary of the fiscal year 2004 Intelligence Authorization Bill. Following the section-by-section analysis and explanation is a more detailed discussion of the provisions contained in the Bill and of the Committee's related comments.

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 lists the U.S. Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for fiscal year 2004.

Section 102. Classified schedule of authorizations

Section 102 makes clear that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities and applicable personnel ceilings covered under this title for fiscal year 2004 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, to the Permanent Select Committee on Intelligence of the House of Representatives, and to the President.

Section 103. Personnel ceiling adjustments

Section 103 authorizes the Director of Central Intelligence, with the approval of the Director of the Office of Management and Budget (OMB), in fiscal year 2004 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 Director of Central Intelligence 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.

Section 104. Intelligence Community Management Account

Section 104 authorizes appropriations for the Community Management Account (CMA) of the Director of Central Intelligence and sets the personnel end-strength for the Intelligence Community Management Staff (CMS) for fiscal year 2004.

Subsection (a) authorizes appropriations of $198,390,000 for fiscal year 2004 for the activities of the CMA of the Director of Central Intelligence. Subsection (a) also authorizes funds identified for advanced research and development to remain available for two years.

Subsection (b) authorizes 310 full-time personnel for elements within the CMA for fiscal year 2004 and provides that such personnel may be permanent employees of the CMA element or detailed from other elements of the U.S. Government.

Subsection (c) authorizes additional appropriations and personnel for the CMA as specified in the classified Schedule of Authorizations and permits the additional funding for research and development to remain available through September 30, 2005.

Subsection (d) requires that, except as provided in section 113 of the National Security Act of 1947, personnel from another element of the U.S. Government be detailed to an element of the CMA on a reimbursable basis, or for temporary situations of less than one year on a non-reimbursable basis.

Subsection (e) authorizes $37,090,000 of the amount authorized in subsection (a) to be made available for the National Drug Intelligence Center (NDIC). Subsection (e) requires the Director of Cen-

tral Intelligence 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. Incorporation of reporting requirements

Section 105 incorporates reporting requirements in the conference report to the Act, and the House and Senate reports on the associated Bills, and the classified annexes thereto, into the Act.

Section 106. Preparation and submittal of reports, reviews, studies, and plans relating to intelligence activities of Department of Defense or the Department of Energy

Section 106 governs preparation and submittal of reports relating to Department of Defense (DoD) or Department of Energy (DoE).

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Authorization of Appropriations

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $226,400,000 for fiscal year 2004 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL PROVISIONS

Subtitle A—Recurring General Provisions

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

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

Section 302. Restriction on conduct of intelligence activities

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

Subtitle B—Intelligence

Section 311. Modification of authority to obligate and expend certain funds for intelligence activities

Section 311 amends the National Security Act of 1947 by removing the "unforeseen requirements" criterion from section 504(a)(3)(B) of the Act (50 U.S.C. 414(a)(3)) (relating to the funding of certain intelligence activities by reprogramming).

Section 312. Modification of notice and wait requirements on projects to construct or improve Intelligence Community facilities

Section 312 amends section 602 of the Intelligence Authorization Act for Fiscal Year 1995 (Public Law 103–359) to change unprogrammed construction notice and wait periods and to raise notification thresholds for certain construction and renovation projects. Section 312(b) amends section 602(b)(2) of the Act to authorize the Director of Central Intelligence and Secretary of Defense to initiate within seven days (vice 21 days) of congressional notification unprogrammed construction projects in excess of the amount specified in section 602(a) of the Act. The provision separately authorizes, in emergencies, commencement of construction immediately upon notification despite the 7-day waiting period that would normally apply, subject to a joint Director of Central Intelligence-Secretary of Defense determination that "an emergency relating to the national security or the protection of health, safety, or environmental quality exists and that delay would harm any or all of those interests." For projects that primarily concern subsection (b)(3) authorizes the Director of Central Intelligence to make the required determination unilaterally.

Section 313. Use of funds for counterdrug and counterterrorism activities for Colombia

Section 313 authorizes the use of funds designated for intelligence or intelligence-related purposes for assistance to the Government of Colombia for counterdrug activities for fiscal year 2004 (and any unobligated funds designated for such purposes for prior years) to be utilized to support a unified campaign against narcotics trafficking and against activities by organizations (such as the Revolutionary Armed Forces of Colombia (FARC), the National Liberation Army (ELN), and the United Self-Defense Forces of Colombia (AUC)), and to take actions to protect human health and welfare in emergency circumstances, including undertaking rescue actions. A similar provision was enacted as Section 501 of the Intelligence Authorization Act for Fiscal Year 2003 (Public Law 107–306).

Section 314. Pilot program on analysis of signals and other intelligence by intelligence analysts of various elements of the Intelligence Community

Section 314 requires the National Security Agency (NSA) to develop a pilot program to improve the ability of analysts in other intelligence agencies to obtain access to and analyze data collected and held by NSA while retaining appropriate handling safeguards.

Section 315. Pilot program on training for intelligence analysts

Section 315 proposes that a Reserve Officers Training Corps (ROTC)-like Intelligence Analyst Program be established by the Assistant Director of Central Intelligence for Analysis and Production (ADCI/A&P). The goal of the program should be to recruit entry-level analysts and operations specialists with enhanced analytic and foreign language skills who are committed to a career in the Intelligence Community.

Section 316. Extension of National Commission for the Review of the Research and Development Program of the United States Intelligence Community

Concerning Section 316, because of military operations to disarm Iraq, Senate organizational issues, and other priorities, the Senate leadership has not yet appointed Commission members. This section extends the Commission to permit appointment of members and commencement of the Commission's duties.

Subtitle C—Surveillance

Section 321. Clarification and modification of sunset of surveillance-related amendments made by USA PATRIOT Act of 2001

Regarding Section 321(a) of this measure, it should be recalled that Section 224 of the USA PATRIOT Act of 2001 (Public Law 107–56 (Oct. 26, 2001)) contained language that would terminate certain provisions of that Act on December 31, 2005. Section 224 clearly assumed, but did not explicitly provide, that the pre-existing text of laws modified by the Act would be restored upon operation of this "sunset" clause. This has raised some concern on account of the provisions of 1 U.S.C.108, which provides as a general rule of statutory construction that "[w]henever an Act is repealed, which repealed a former Act, such former Act shall not thereby be revived, unless it shall be expressly so provided." The Committee believes that because the USA PATRIOT Act "sunset" clause does not involve the "repeal" of actual "Acts," that 1 U.S.C. 108 would in all likelihood not affect the coherence of Section 224 of the Act. Nevertheless, in order to provide absolute clarity, the Committee provides in this section that laws modified by those sections of the USA PATRIOT Act listed in Section 224 will return to their pre-USA PATRIOT Act form after the operation of the "sunset" provision.

Section 216 of the USA PATRIOT Act modified authorities relating to the use of pen registers and trap and trace devices. Section 204 of the Act clarified that intelligence exceptions continued to apply to limitations on the interception and disclosure of wire, oral, and electronic communications, notwithstanding the modifications of Section 216. Section 224 of the Act contains a sunset provision that excludes section 216, but includes section 204. This omission of Section 204 from the sections excluded from "sunset" creates a technical anomaly. Section 321(b) corrects the technical oversight and removes Section 204 of the Act from the sunset provision. If not removed, valuable and necessary intelligence exemptions to the pen register and trap and trace provision would be lost after December 31, 2005.

Subtitle D—Reports

Section 331. Report on cleared insider threats to classified computer networks

Section 331 requires the Director of Central Intelligence, in conjunction with the Secretary of Defense, to provide, in a one-time report to Congress, an assessment of the national security risks posed by "cleared insiders" that are inherent in current computer security practices within the Intelligence Community and DoD.

Section 332. Report on security background investigations and security clearance procedures of the Federal Government

Section 332 requires the Director of Central Intelligence, in coordination with the Secretary of Defense, to provide a report on the adequacy and future direction of security background investigations and clearance procedures within the U.S. Government.

Section 333. Report on detail of civilian intelligence personnel among elements of the Intelligence Community and the Department of Defense

Section 333 requires the Director of Central Intelligence, in conjunction with the Secretary of Defense, to provide an assessment to Congress of ways to ease movement of civilian intelligence personnel between various elements of the Intelligence Community to respond more flexibly and effectively to the shifting needs of intelligence collection and analysis.

Section 334. Report on modifications of policy and law on classified information to facilitate sharing of information for national security purposes

Section 334 requests that the President review Executive Orders 12333 and 12598 and submit a report within 6 months on potential changes to the Executive Orders or legislative actions which could be applied to facilitate information sharing and data access across the Intelligence Community.

Section 335. Report of Secretary of Defense and Director of Central Intelligence on strategic planning

Section 335 requires the Secretary of Defense and the Director of Central Intelligence, jointly, to report not later than February 15, 2004, on progress toward establishing an independent, comprehensive, analytical capability to assess collection program alternatives, as well as the steps taken to better coordinate DoD and Intelligence Community strategic planning.

Section 336. Report on United States dependence on computer hardware and software manufactured overseas

Section 336 directs the Director of Central Intelligence to prepare a thorough evaluation of the trends and the strategic implications of increasing United States reliance on foreign hardware and software.

Section 337. Report on lessons learned from military operations in Iraq

Section 337 requires the Director of Central Intelligence to submit a report regarding intelligence lessons learned as a result of Intelligence Community support to military operations during the course of Operation Iraqi Freedom. The report must be submitted to the appropriate committees not later than one year after enactment of this Act.

Section 338. Reports on conventional weapons and ammunition obtained by Iraq in violation of certain United Nations Security Council resolutions

Section 338 requires the Director of the Defense Intelligence Agency (DIA), not later than 120 days after the cessation of hostilities in Iraq, to submit a preliminary report to certain specified committees regarding conventional weapons and ammunition obtained by Iraq in violation of applicable United Nations resolutions. A final report is required not later than 270 days after the cessation of hostilities in Iraq. Given the May 1, 2003 remarks by the President concerning the conclusion of major combat operations in Iraq, the Committee believes there has been a cessation of hostilities in Iraq as of that date for purposes of this reporting requirement.

Section 339. Repeal of certain report requirements relating to intelligence activities

Section 339 eliminates certain reporting requirements that no longer have enough utility in the legislative oversight process to justify the burdens they impose upon intelligence agencies that are hard at work protecting the United States against international terrorism, supporting our troops in combat in Iraq and Afghanistan, and otherwise safeguarding and advancing our national security. This section identifies a number of reports for elimination.

Subtitle E—Other Matters

Section 351. Extension of suspension of reorganization of Diplomatic Telecommunications Service Program Office

Section 351 extends for an indefinite period the suspension authorized in section 311 of the Intelligence Authorization Act for fiscal year 2002, Public Law 107–108 (Dec. 28, 2001), and extended by section 351 of the Intelligence Authorization Act for Fiscal Year 2003, Public Law 107–306 (Nov. 27, 2002). Section 311 of the Intelligence Authorization Act for Fiscal Year 2002 suspended the provisions of the Intelligence Authorization Act for Fiscal Year 2001 (22 U.S.C. 7301 et seq.) that required reorganization of the Diplomatic Telecommunications Service Program Office (DTS–PO). Section 315 of this Act extends the suspension until 60 days after the appropriate congressional committees are notified by the Secretary of State or the Director of OMB, or the Director's designees, that the present operating framework for the DTS–PO has been terminated. In designating officials under this section, the Committee expects that the Director of OMB shall designate at least those officials referenced in the Classified Annex to this Bill.

Section 352. Modifications of authorities on explosive materials

Section 352 amends the Safe Explosives Act, Public Law 107–296, Secs. 1121–28 (Nov. 25, 2002), to ensure that the provision provides sufficient authority for the Secretary of Defense and the Director of Central Intelligence to conduct, respectively, authorized military and intelligence activities of the U.S. Government. In addition, the provision makes minor technical corrections to certain other provisions in the Act.

Section 353. Modification of prohibition on the naturalization of certain persons

Section 353 amends section 313(e)(4) of the Immigration and Nationality Act (8 U.S.C. 1424(e)(4)), bringing the provision into essential conformity with the determination process established in comparable provisions of law governing the admission or expedited naturalization of certain aliens and their immediate family members, based on the alien having contributed to the national security or intelligence mission of the United States. Under section 7 of the Central Intelligence Agency Act of 1949 (CIA Act) (50 U.S.C. 403h), section 316(f) of the INA (8 U.S.C. 1427(f)), and section 305 of Public Law 104–293 (Oct. 11, 1996) (8 U.S.C. 1427 note), admission determinations regarding an alien's national security or intelligence mission contribution are made by the Director of Central Intelligence, the Attorney General, and (formerly) the Commissioner of Immigration and Naturalization. Unlike those provisions, section 313(e)(4) requires consultation with the Secretary of Defense. This difference from comparable determination processes has created implementation difficulties. This amendment to section 313(e)(4) leaves the determination process to the Director of Central Intelligence, the Attorney General, and the Secretary of Homeland Security, reflecting the transfer of responsibility for adjudication of naturalization petitions from the Commissioner of Immigration and Naturalization to the Department of Homeland Security. See Homeland Security Act of 2002, Public Law 107–296 (Nov. 25, 2002). The Secretary of Defense may still request the naturalization of a particular alien by forwarding to the Director of Central Intelligence the names of aliens who have made a national security or intelligence contribution to DoD. Moreover, when DoD activities are relevant to the determination, consultation with the Secretary of Defense would still be required.

Section 354. Modification to definition of financial institution in the Right to Financial Privacy Act

Section 354 provides enhanced authority for authorized Intelligence Community collection activities designed to prevent, deter, and disrupt activities directed against the United States. This section expands the definition of "financial institution" for purposes of section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414). Section 1114 currently permits U.S. Government authorities engaged in counterintelligence or foreign intelligence activities to obtain certain financial records. The definition of "financial institution" in the Right to Financial Privacy Act—essentially unmodified since the Act became law in 1978—significantly excludes certain entities that provide financial services to the public. Financial records maintained by these entities are not covered by the Act and, thus, are not accessible by counterintelligence and foreign intelligence elements of the U.S. Government under the Act, limiting the effectiveness of national security investigations. In order to expand the definition of "financial institution" for purposes only of section 1114, this subsection adopts, in part, the definition of "financial institution" found in section 5312(a)(2) of title 31, United States Code. The expansion of this definition is consistent with the definition used in section 804(5) of the Counterintelligence and Se-

curity Enhancements Act of 1994, Public Law 103–359 (50 U.S.C. 438).

Section 355. Coordination of Federal Government research on security evaluations

Section 355 requires that the National Science Foundation and the Office of Science and Technology jointly submit to Congress a written report identifying the research most likely to advance the understanding of the use of certain assessments of individuals in security evaluations; distinguish between short-term and long-term areas of research in order to maximize the utility of short-term and long-term research on such assessments; identify the Federal agencies best suited to support such research; and develop recommendations for coordinating future Federally-funded research for the development, improvement, or enhancement of security evaluations.

Section 356. Technical Amendments

Section 356 corrects now-erroneous citations to section 103(c)(6) of the National Security Act of 1947 (50 U.S.C. 403–3(c)(7)), which was redesignated section 103(c)(7) by section 901 of the USA PATRIOT Act of 2001, Public Law 107–56 (Oct. 26, 2001), thus necessitating the technical correction made by this section. This section also corrects incorrect cross-references in Section 15 of the CIA Act (50 U.S.C. 403o) and Section 11 of the National Security Agency Act of 1959 (50 U.S.C. 402 note) to the authorities of the General Services Administration (GSA) special policemen. The authorities of GSA special policemen were transferred to "officers and agents of the Department of Homeland Security" pursuant to Section 1706(b)(1) of the Homeland Security Act of 2002, Public Law 107–296 (Nov. 25, 2002) (40 U.S.C. 1315). This section provides technical corrections to the referenced statutes.

TITLE IV—CENTRAL INTELLIGENCE AGENCY

Section 401. Amendment to certain Central Intelligence Agency Act of 1949 notification requirements

Section 401 amends the CIA Act (50 U.S.C. 403e(b)(5)) to exempt section 4(b)(1) implementing regulations from the prior notification requirements of section 4(b)(5). To the extent the Central Intelligence Agency (CIA) adopts unique allowances and benefits under section 4(b)(2) or (b)(3) or adopts or modifies regulations under section 4(b)(4), notification of the Intelligence Committees prior to implementation is still required.

Section 402. Protection of certain Central Intelligence Agency personnel from tort liability

Section 402 provides protections from tort liability for certain specified CIA personnel (and, with respect to specified NSA personnel, Section 502) when those personnel take reasonable action, including the use of force, (1) to protect an individual in their presence from a "crime of violence", (2) to assist an individual who has suffered, or is threatened with, bodily harm, or (3) to prevent the escape of an individual who the personnel reasonably believe to have committed a crime of violence in their presence.

Section 403. Repeal of obsolete limitation on use of funds in Central Services Working Capital Fund

Section 403 modifies the CIA Central Services Program (CSP) by removing the technically expired requirements of section 21(f)(2)(B) of the CIA Act (50 U.S.C. 403u(f)(2)(B)).

Section 404. Technical amendment to Federal Information Security Management Act of 2002

Section 404 is a technical amendment to the Federal Information Security Management Act of 2002. Section 1001(b)(1) of the Homeland Security Act of 2002 and Section 301(b)(1) of the E–Government Act of 2002 amended title 44, United States Code, to require an annual independent evaluation of information security programs. As enacted, only an Inspector General created by the Inspector General Act of 1978 or an independent external auditor may perform the evaluation required by these provisions. Section 404 clarifies that Inspectors General authorized by other statutes (e.g., Section 17 of the CIA Act (50 U.S.C. 403q)) may also perform the required evaluation.

TITLE V—DEPARTMENT OF DEFENSE INTELLIGENCE MATTERS

Section 501. Protection of operational files of the National Security Agency

Section 501 allows the Director of NSA, in coordination with the Director of Central Intelligence, to exempt certain operational files of NSA from search and review under the Freedom of Information Act (FOIA), 5 U.S.C. 552. This section would allow exemptions for files concerning the activities of NSA that document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems. This exemption authority parallels that currently enjoyed by CIA, the National Imagery and Mapping Agency (NIMA), and the National Reconnaissance Office (NRO).

Section 502. Provision of affordable living quarters for certain students working at National Security Agency laboratory

Section 502 amends section 2195 of title 10, United States Code, to permit the Director of NSA to provide and pay for living quarters for Cooperative Education Program and Summer Program students to address an existing housing shortage.

Section 503. Protection of certain National Security Agency personnel from tort liability

Section 503 provides protections from tort liability for certain designated NSA personnel when those personnel take specified actions. The protections are similar to those afforded certain CIA personnel under Section 402.

Section 504. Authority for Intelligence Community elements of Department of Defense to award personal service contracts

Section 504 provides authority for Intelligence Community elements of DoD to award personal services contracts, similar to the CIA's existing authority for personal services contracts under Section 8 of the CIA Act (50 U.S.C. 403j(a)(1)).

COMMITTEE COMMENTS ON FISCAL YEAR 2004 INTELLIGENCE AUTHORIZATION BILL AND OTHER MATTERS

The Committee is mindful of the many sacrifices over the last year made by members of the Intelligence Community around the world. The Committee expresses its profound gratitude to them, and offers its heartfelt condolences to the families of those who made the supreme sacrifice.

INTELLIGENCE COMMUNITY MANAGEMENT, PLANNING, AND PERFORMANCE

The Committee has been vigilant and will continue to vigorously oversee the management, planning, and performance of the Intelligence Community. We have grown concerned with—and the Administration has continually raised—the issue of bureaucratic impediments to the prosecution of the important national security mission of the Intelligence Community. To address these impediments, the Committee has repealed or modified statutory requirements on the Intelligence Community that no longer serve a legitimate oversight purpose, are unnecessary obstacles to the implementation of new initiatives, or fail to account for the passage of time. The Committee remains concerned, however, with several management issues still unresolved by the Intelligence Community.

Intelligence Community strategic and performance planning

Fiscal year strategic and performance plans

For the last two fiscal years, the Committee has expressed in its report language an interest in strategic and performance planning within the Intelligence Community. In response, the CMS in 2002 submitted strategic and performance plans for the Intelligence Community as a whole, as well as for selected agencies within the National Foreign Intelligence Program (NFIP). These documents were the first-ever plans coordinated across the Intelligence Community aimed at establishing performance measures aligned with the stated goals and priorities of the Director of Central Intelligence.

While the Committee was pleased with this first effort by CMS and the Intelligence Community, Senate Report 107–149 contained suggestions for improvements to future reports. Specifically, the Committee was concerned that the Intelligence Community's initial performance plans focused more on increasing intelligence capabilities than on the value that such capabilities would add to achieving the Intelligence Community's missions. As such, the Committee directed that the fiscal year 2004 performance plans include "mission-based" performance measures linking Intelligence Community capabilities to the stated strategic goals of the Director of Central Intelligence. The Committee believes that these mission oriented performance measures should complement the budget process within the CMS and the agencies within the NFIP. For this reason, the Committee also directed that the fiscal year 2004 performance plans include specific information on how the agencies utilized them in preparing their respective sections of the fiscal year 2004 budget for the NFIP.

On February 25, 2003, the CMS submitted to the Committee the Fiscal Year 2004–2009 Intelligence Community Strategy, as well as

the strategies for the component agencies. The Committee, however, has yet to receive an updated Intelligence Community performance plan for fiscal year 2004 and has received only two fiscal year 2004 performance plans for individual Intelligence Community components. These documents were due to Congress by March 1, 2003. Although the Committee understands that the CMS is still editing and revising the performance plans submitted by the component agencies, no extension of the March 1, 2003, deadline has been requested. The Committee is disappointed that the Intelligence Community has not completed these valuable documents in time to support the Committee's authorization for this fiscal year or to inform the Intelligence Community's own planning processes. The Committee looks forward to receiving the performance plans and expects that CMS will submit them in the near future. Before submitting these reports, CMS should coordinate their efforts with the office of the Under Secretary of Defense for Intelligence to ensure that requirements in CMS performance reports do not conflict with commitments that Intelligence Community agencies within DoD make as part of the DoD strategic and performance planning processes.

Strategic planning for sensors and platforms

The Committee is aware of no capability within DoD or the Intelligence Community for objectively, independently, and comprehensively evaluating alternative sensor and platform architectures and capabilities. There are some capabilities within different agencies and departments, but none that are available, independent of the program offices, to model and assess cross-program trades without regard to the location of the sensor or platform (air, space, land, or sea) or the level of compartmentation. Consequently, although DoD and Intelligence Community officials expend substantial effort and time evaluating program trades, they do so without the benefit of the rigorous quantitative modeling necessary to optimize collection capabilities and architectures. Given the vast sums involved in these programs, even modest increases in the efficiency of resource allocation could lead to substantial benefits. Further, the Committee notes that the national military strategy, as well as the Defense Planning Guidance, have been developed in recent years without the participation of the Director of Central Intelligence or his staff, notwithstanding the growing importance of intelligence to military operations and the need to build forces commensurate to validated threats.

Accordingly, in Section 335, the Committee requires the Secretary of Defense and the Director of Central Intelligence to jointly report on progress toward establishing an independent, comprehensive, analytical capability to assess collection program alternatives, as well as the steps taken to better coordinate DoD and Intelligence Community strategic and budgetary planning.

Intelligence Community compliance with Federal financial accounting standards

In Senate Report 107–63, the Committee conveyed its concern with the Intelligence Community's financial management practices and required the Director of Central Intelligence and the Secretary of Defense to task the appropriate statutory Inspectors General to

perform an audit of the form and content of the Fiscal Year 2001 financial statements of NSA, DIA, NIMA, and CIA. This audit was designed to ascertain if these agencies were able to produce financial statements that met Federal Government financial accounting standards and OMB requirements. The NRO was not included in this requirement because its financial statements have been audited by an independent public accounting firm for the past three years.

The resulting DoD and CIA Inspectors General reports found that NSA, DIA, NIMA, and CIA could not produce auditable financial statements. Among the faults depicted were the improper preparation of selected required statements, failure to use accrual accounting, inability to reconcile the fund balance with Treasury, and inaccurate reporting of property, plant, and equipment. The Committee found the lack of internal controls reflected by these problems of great concern.

Senate Report 107–63 also mandated that the Director of Central Intelligence, in consultation with the Secretary of Defense, should ensure that NSA, DIA, NIMA, and CIA all receive an audit of their financial statements no later than March 1, 2005, to be executed by a statutory Inspector General or a qualified independent public accountant. The Committee acknowledged that NSA, DIA, and NIMA may be affected by DoD plans to implement a DoD-wide Financial Management Modernization Program, which is not expected to be completed before 2007. For example, the DoD Inspector General noted that NSA halted its plan to purchase a compliant accounting system based on guidance from the Under Secretary of Defense (Comptroller). This, in turn, affected DIA and NIMA, which both use portions of the NSA accounting system.

In Senate Report 107–149, to facilitate adequate oversight of the Intelligence Community's financial management systems and practices, the Committee directed that the Deputy Director of Central Intelligence for Community Management provide the Intelligence Committees with a report on how CMS is structured to monitor Intelligence Community compliance with the Chief Financial Officers Act and related OMB guidance. The report recently provided to the Committee by CMS included plans to monitor the ability of each agency to produce a financial statement audit by 2005 and a description of the ability of CMS to assess the financial systems of each agency in order to generate required oversight information.

Prior to the 2005 audit requirement, and as follow-on to the initial Inspectors General reports, Public Law 107–306 contained a statutory requirement for annual reports from each agency head describing the activities their organization had undertaken to produce auditable financial statements. Additionally, the annual agency reports required by Public Law 107–306 were to include a description of the impact of the DoD modernization program and the steps being taken to make current systems compliant with Federal standards in the interim. As of this writing, no such report has been received from NSA, DIA, NIMA, or CIA. The Committee notes that, due to the shift of certain report due dates in Public Law 107–306, some confusion existed as to the actual due date of these reports. CMS recently coordinated interim responses from the subject agencies. The Committee, however, is concerned that this initial failure to consult the Committee on the due date is an indica-

tion that the Intelligence Community still lacks the appropriate level of interest in responsible financial management.

While the Committee has not received direct agency responses, it notes that the DoD Inspector General independently provided the Committee with follow-up reports that addressed the soundness of the fiscal year 2002 financial statements of DIA and NIMA, as well as the adequacy of their related procedures and controls. The DoD Inspector General found that the financial statements of these agencies were still unreliable. The reports determined that neither agency dedicated the proper resources to the financial management and reporting function and had not addressed the lack of internal controls or deficiencies related to reconciling the data contained in the various financial statements. The reports noted that the existing noncompliant budgeting systems and the current DoD financial management modernization program hampered the agencies. The DoD Inspector General recommended that the agencies institute improved internal control procedures and devote the appropriate resources toward the preparation of financial statements that will meet OMB and DoD standards. A similar follow-up report on NSA is in progress.

The CMS report on its oversight capabilities noted that the respective DoD agency heads, not the Director of Central Intelligence, have direct financial management authority and responsibility for their agencies. Thus, the agency directors, not the CMS, should provide the annual reports describing the activities that each agency has undertaken to produce auditable financial statements. Furthermore, in response to known difficulties in acquiring the systems necessary to produce financial statements, the Committee has indicated its willingness to address the issue of extending the 2005 audit requirement. However, in the absence of the required progress reports from the directors of NSA, DIA, NIMA, and CIA, the Committee has elected to delay a decision on the deferral of the 2005 audits, pending the receipt of these progress reports by December 1, 2003. The Committee has recently learned that a decision on the contractor for the new DoD financial management architecture is forthcoming. In light of this imminent selection, the Committee believes the December 1, 2003 deadline will provide the agencies with ample time to assess the impact of the new architecture.

National Security Agency budget, acquisition, and compensation reform

Congressional Budget Justification Book

The Committee commends the Director of NSA for the progress made in the presentation and format of the Congressional Budget Justification Book (CBJB) for the Administration's request for fiscal year 2004. When compared to previous submissions, NSA's CBJB represents a good faith effort to project to Congress an accurate, comprehensible request. The new budget structure and attendant cross-walk, while complex, are understandable. Much remains to be done, but the progress displayed in this single year is noteworthy.

Acquisition

The Committee continues to be concerned with the state of the NSA acquisition process and frustrated by the lack of progress realized in remedying this problem over the past three years. The Administration's budget request sustains the long overdue increase for the Consolidated Cryptologic Program (CCP) executed by NSA. Last year's significant increase over the previous year coupled with the fiscal year 2004 requested increase, will allow NSA to continue its transformation initiative while supporting the global war on terrorism and the war to liberate Iraq. These significant investments will lead to major acquisition programs designed to modernize the Signals Intelligence (SIGINT) enterprise for the future. The lack of a fundamentally sound acquisition process, however, raises concerns with respect to the efficiency and execution of these major acquisitions.

The Committee's concern with the health of the NSA acquisition process is not new. In both fiscal year 2002 and 2003, the Committee noted significant shortfalls and recommended actions that would correct the documented deficiencies. In both the Fiscal Year 2002 and 2003 Intelligence Authorization Act Conference Reports, lack of a credible NSA acquisition process was noted, along with several recommendations for corrective actions. While NSA has made modest progress in some of the various components of a good acquisition process, reports from oversight departments within the Administration point out one glaring fault in the road to progress: the authority of the NSA Senior Acquisition Executive (SAE) is not commensurate with that needed to empower him to take the necessary actions to correct even the most elementary deficiencies. The NSA SAE has not been given the requisite authority by the Director of NSA to bring the agency's acquisition process up to acceptable DoD standards.

In June 2000, the SAEs for the Intelligence Community and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), in response to a Congressionally Directed Action (CDA), provided a report titled "Independent Review of the National Security Agency Acquisition Process", which they have updated on a periodic basis. These reviews have covered nine specific components that can contribute to attaining the DoD standard for acquisition performance. The review is metrics based. The nine categories are evaluated on a "red, yellow, green" criteria and an assessment measurement has been added for implementation. While marginal progress has been noted, none of the nine criteria has yet to be judged fully green, and none of the implementation ratings is above 2 on a 1–4 scale. After three years, the average for the nine categories is "yellow—Process and Structure Identified." The average assessment is 1.4, with the definition of a 2 rating being "Process immature; inconsistent application or effectiveness." A rating of 1 is defined as "Process ineffective or limited acceptance and practice." Perhaps the most glaring area reviewed is titled "Establish a dedicated SAE reporting directly to the [Director of NSA]." This category actually moved down from "Yellow/Green" to "Yellow" over the last evaluation period and is judged to be at implementation level 1. Establishing an NSA SAE that reports directly to the Director of NSA can be remedied easily, and the fact that the rating associated with this component has moved

backward is of great concern to the Committee. To hire the very best NSA SAE is commendable; to deny that individual the necessary authority to make a difference is an opportunity missed.

The Committee recommends that the Director of NSA take the following actions immediately: (1) Clarify the lines of authority to and responsibility of the NSA SAE for program execution; (2) Align Program Manager (PM) and Acquisition Program Manager (APM) acquisition responsibilities under the NSA SAE; (3) Establish clear budgetary authority for the NSA SAE over all budgets associated with major acquisition programs; (4) Establish clear reporting and evaluation lines from the PMs and APMs to the NSA SAE; (5) Provide the NSA SAE true management power over the acquisition decision process. The requirement for acquisition decisions to be made by consensus must be eliminated. Acquisition management groups made up of non-acquisition professionals must be made advisory only, and the NSA SAE must not be forced to form a consensus within these groups to enable an acquisition decision.

The Committee greatly appreciates the efforts by CMS and DoD to remedy this problem and requests that an update to the February 2003 report be submitted to the Committee no later than August 30, 2003.

Acquisition baseline

For the past two years, the Committee has made an issue of the inadequacy of the NSA acquisition baseline. It is very difficult for the Committee to understand what needs to be done to modernize NSA when NSA cannot provide an adequate baseline of ongoing development and acquisition programs, projects, and activities. A great deal of funding has been appropriated to NSA over the past year, and there is little doubt that more will be required to ensure that the country has the very best SIGINT capability in the world. The results witnessed during the ongoing global war on terrorism and the support provided to our troops in Iraq has been excellent. But our successes will not be lost on future enemies, and the threat will evolve to defeat our present capabilities. Transformation is expensive, and the Committee wants to support the Director of NSA in this effort, but without the knowledge of what is actually being funded at NSA, it is difficult to sustain support for increasing levels of authorization.

The Committee has fenced funds over the past two fiscal years to try to bring command attention to this problem. Submissions to date have shown progress, but are not comprehensive in identifying known projects and programs that are being funded in the CCP. Several projects listed in the CBJB requesting continued funding in fiscal year 2004 are not currently listed in the project baseline provided to the Committee. It is imperative that the baselining effort be put under competent, empowered authority with clear direction to develop a complete and comprehensive baseline. Future funding requests will be balanced against the NSA acquisition baseline so it is in the agency's best interest to get this done right, and soon.

The Committee directs NSA, beginning the first quarter of fiscal year 2004, to submit quarterly to the Committee a document baselining all programs, projects, and activities ongoing within the CCP. This document should be prepared by the NSA SAE in con-

junction with the Chief Financial Manager—the only two authorities below the Director of NSA who have the ability to validate, track, and link NSA programs, projects, and activities to acquisition schedules and funding authorizations. These quarterly reports will integrate each entry in the baseline to a master schedule and link the various entries showing dependencies and functional similarities. Specific requirements will be listed with the entries such that customer relationships are understood and definable. Ideally, the NSA acquisition baseline can be fully automated and put online so that all members of the SIGINT enterprise can understand what projects, programs, and activities are ongoing to reduce redundancies and facilitate technology exchange. Rates of expenditures by appropriations will be reflected in these quarterly submissions.

Menwith Hill Station

The Committee is encouraged by the budgetary increase requested to improve the condition of the facilities and infrastructure at Menwith Hill Station. There may be an opportunity to improve these conditions even further with a process known as the "Public Private Partnership"—a process used effectively by other organizations in the United Kingdom. This acquisition method is used to establish a long-term contract for acquiring, building, and updating facilities and could benefit both infrastructure and mission support. The "Public Private Partnership" is frequently coupled with a "Private Financing Initiative" that leverages private financing to provide capital funding for infrastructure projects. In the United Kingdom, the Ministry of Defence is moving positively to this acquisition method and the method might have considerable benefit to United States interests in the United Kingdom, as well.

The Committee directs that the Director of NSA review the "Public Private Partnership"—and the "Private Financing Initiative" concepts for application to Menwith Hill Station and report to the Committee the findings of the review no later than June 13, 2003. The report should describe the benefits of this approach, identify any potential issues, and recommend whether this acquisition method should be executed by the U.S. Government. The report should capitalize on the experience gained by the host government, particularly the experiences of the General Communications Headquarters (GCHQ) in their recent initiatives in this regard. The review will be coordinated with the U.S. Executive Agent for the United Kingdom and the on-going Menwith Hill Transition Team.

National Security Agency Compensation Reform

The NSA has briefed the Committee on the proposed implementation of its new Compensation Reform Plan. Changing compensation systems is difficult in any work force, and the Committee is pleased to see that the NSA leadership has taken the time to ensure that all employees are informed of the need for change and of the impacts on them of the new system. As a necessary precursor to any new compensation plan, the Committee has supported the implementation of a new employee performance evaluation mechanism. The Committee strongly believes that any new evaluation mechanism should be implemented at least a year before initiation of a revised compensation plan. The Committee will

closely follow both the implementation of the new employee performance evaluation mechanism and the initiation of the pilot compensation reform initiative at NSA.

Defense Finance and Accounting Service and the National Security Agency

The NSA is making progress in its financial and accounting practices. Additional work remains to be done, however, and resources will be required to modernize this critical part of the NSA business practice.

The Committee has been advised that the Defense Finance and Accounting Service (DFAS) is considering moving certain aspects of the NSA support centers to a centralized accounting and finance structure under the control of DFAS. The Director of NSA is making progress in modernizing his business practices. Separation of the finance function from his authority would not support the overall objectives of this Committee to improve the acquisition business area at NSA. Therefore, the Committee directs that DFAS brief the Committee before any transfer of authority, personnel, or resources is considered or affected.

The Deputy Director of Central Intelligence for Community Management will notify the Committee of any efforts by DFAS to transfer accounting or finance authorities from any NFIP components prior to such transfer. No transfer will be affected without the approval of this Committee.

Authority for Intelligence Community elements of Department of Defense to award personal service contracts

Intelligence Community elements of DoD frequently have a temporary need for additional personnel with specific expertise to meet unanticipated, yet significant, operational requirements that necessitate a bolstering of organizational and personnel efforts created by world events. Current examples include experts on al-Qa'ida, the countries of the Middle East, chemical and biological warfare, and Islamic militant personalities, along with linguists to support interrogation of detainees and review of captured documents. Under current law, U.S. Government agencies generally must choose between hiring additional personnel as government employees or contracting for their services under the restrictive provisions for the temporary or intermittent employment of experts and consultants under section 3109 of title 5, United States Code. The Committee provides relief from these more restrictive authorities by granting authority for Intelligence Community elements of DoD to award personal services contracts notwithstanding any other provision of law. This authority is similar to that already exercised by CIA under Section 8 of the CIA Act (50 U.S.C. 403j(a)(1)). This provision will optimize the capabilities of Intelligence Community elements of DoD in the performance of their roles in the global war on terrorism and in the execution of future national security missions.

Report on detail of civilian intelligence personnel throughout the Intelligence Community

The Committee is aware that DoD uses a system for quickly and rapidly moving Senior Executive Service employees from one com-

ponent to another to respond flexibly and effectively to shifting needs and to implement policy guidance from seniors. The Committee believes that the Intelligence Community should study a similar system. To that end, Section 333 requires the Director of Central Intelligence, in conjunction with the Secretary of Defense, to provide an assessment to Congress of ways to ease movement of civilian intelligence personnel between the various elements of the Intelligence Community to respond to the shifting needs of intelligence collection and analysis.

Protection of certain Intelligence Community personnel from tort liability

Specified law enforcement and Diplomatic Security Service officers are provided protections from tort liability pursuant to section 627 of the Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1999 (Public Law 105–277) when they take reasonable action, including the use of force, (1) to protect an individual in their presence from a "crime of violence", (2) to assist an individual who has suffered, or is threatened with, bodily harm, or (3) to prevent the escape of an individual who the personnel reasonably believe to have committed a crime of violence in their presence. The Committee extends these protections from tort liability to certain specified personnel of CIA and NSA. When these highly trained CIA and NSA professionals are on official duty and take reasonable actions to protect and aid individuals in their presence, they should not be deprived of protections from tort liability that other similarly situated personnel of the Federal Government are granted under existing law. In recognition of the current potential exposure of these personnel to tort liability and the protections in law for other personnel of the U.S. Government, the Committee (in Sections 402 and 503) extends the protections of section 627 of Public Law 105–277 to these specified CIA and NSA personnel.

Modification of authority to obligate and expend certain funds for intelligence activities

Section 504 of the National Security Act of 1947 (50 USC 414) requires that funds appropriated to an intelligence agency for an intelligence or intelligence-related activity may be obligated or expended only if such funds are specifically authorized for use for such activities. Although reprogrammings to meet a higher-priority intelligence need are permitted upon notification to the Intelligence Committees, Section 504(a)(3)(B) also mandates that the need be based on "unforeseen requirements." The "unforeseen requirements" criterion in Section 504 tied the hands of Congress and the Intelligence Community in unnecessary and time-consuming legal debates over proposed reprogrammings.

In Section 311 of the Bill, the Committee amends Section 504 to delete the "unforseen requirements" criterion, ensuring that the Intelligence Community—in cooperation with the Intelligence Committees—can react more quickly to confront higher-priority intelligence needs. Elimination of this requirement will permit reprogrammings to be reviewed on the basis of relative needs and priorities. The provision will also provide the Intelligence Community and Congress with flexibility to resolve differences between

funds appropriated for intelligence and intelligence-related activities but not specifically authorized, and vice versa.

Modification of notice and wait requirements on projects to construct or improve intelligence community facilities

Section 602 of the Intelligence Authorization Act for Fiscal Year 1995, Public Law 103–359 (Oct. 14, 1994) (50 U.S.C. 403–2b) placed certain notification requirements for unprogrammed Intelligence Community construction and renovation projects. Since passage of the original notification requirements over eight years ago, construction costs have grown steadily—particularly those costs related to security and information technology. Moreover, in recognition of the Intelligence Community's need for increased agility to meet shifting threats, the Committee has lowered the "notice-and-wait" period associated with certain unprogrammed construction and renovation projects from 21 days to 7 days and added an additional emergency category in which only notice (and no wait) would be required. The Committee expects that the emergency category would be used only in the most extraordinary circumstances.

Provision of affordable living quarters for certain students working at National Security Agency laboratory

Student programs are essential for NSA to compete in the highly challenging labor market and to ensure that it remains a competitive, prospective employer for students with hard-to-find scientific and technical skills. The single biggest obstacle identified by NSA to the growth of these student programs is a lack of affordable short-term housing in and around NSA. By permitting the Director of NSA to pay for living quarters for certain students in specified NSA programs, Section 502 seeks to ensure that future students are not deterred from seeking a valuable and beneficial employment opportunity with NSA simply because of the unavailability of affordable, short-term housing.

Repeal of certain Intelligence Community reporting requirements

The Committee maintains that ad hoc reporting requirements and other CDAs imposed by Congress upon the Intelligence Community are a vital tool of legislative oversight and are often highly valuable to various committees. Unfortunately, these reporting obligations have proven easier to impose than to remove. As a result, the Intelligence Community has faced ever-increasing reporting burdens, even when the practical utility of specific reports to Congress has largely lapsed. As the reporting burdens multiplied, the fragmented and unsystematic nature of reporting requirements led the Intelligence Community to become lax about fulfilling its obligations to provide the requested reports in a timely and effective manner. In sum, neither Congress nor the Executive Branch was well served by the reporting and CDA process that had developed.

In Title VIII of the Intelligence Authorization Act for Fiscal Year 2003, Congress took steps to rationalize and structure the previously ad hoc reporting process—organizing and incorporating the myriad existing requirements into a single reporting structure, imposing clear deadlines, and reemphasizing that the Intelligence Community is required by law to comply with all such requirements.

The Committee is resolved to building upon prior efforts to bring the reporting/CDA process under control. In this bill, the Committee takes affirmative steps to eliminate reporting requirements that no longer have sufficient utility in the legislative oversight process to justify the burdens imposed upon intelligence agencies hard at work protecting the United States against international terrorism, supporting our troops in combat in Iraq and Afghanistan, and otherwise safeguarding and advancing our national security. Section 339 identifies a number of reports for elimination and changes one semiannual report to an annual report.

Periodic reports are often very important tools of legislative oversight, but there can be no substitute for taking affirmative steps to request information from the Intelligence Community as an everyday part of effective oversight. The Committee anticipates that the elimination of these and other reporting requirements will in no way diminish the vigor of intelligence oversight, will contribute to the Intelligence Community's ability to accomplish its important national security missions, and will not otherwise effect (and will hopefully improve) the Community's willingness to fulfill the day-to-day requests of the Intelligence Committees.

Cancellation of other Intelligence Community reporting requirements

In addition to the modifications to certain statutory reporting obligations, the following reports required to be submitted by Committee reports from previous fiscal years shall be deemed cancelled when the fiscal year 2004 Intelligence Authorization Bill is reported by the Committee. Thereafter, the Executive Branch need not submit:

a. Recurring report(s) on comprehensive annual reviews of customer satisfaction created under "Customer Satisfaction With Intelligence Collection and Analysis and Production," National Foreign Intelligence Program, discussed on p. 4, Senate Report 106–48, Authorizing Appropriations for Fiscal Year 2000 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System and for Other Purposes; and

b. Recurring report on the Intelligence Community's information infrastructure, created under "Assessment of the Intelligence Community's Information Infrastructure" on p. 17, Senate Report 105–185, Authorizing Appropriations for Fiscal Year 1999 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System and for Other Purposes.

Central Intelligence Agency Act of 1949 notification requirements

Section 4(b)(5) of the Central Intelligence Agency Act of 1949

Section 4(b) of the CIA Act (50 U.S.C. 403e(b)(5)) permits CIA to authorize and implement certain allowances and benefits for payment to officers and employees of CIA and to personnel detailed or assigned to CIA. Section 4(b)(5) requires CIA to submit all regulations authorizing allowances and benefits under section 4(b) to the Intelligence Committees prior to implementation. This notification requirement was included to ensure that the Intelligence Commit-

tees were apprised of CIA's use of the broad authority conferred by section 4(b)—particularly with respect to sections 4(b)(2) and (b)(3), which authorize CIA to adopt Agency-unique allowances and benefits under certain circumstances.

Under section 4(b)(1), however, CIA may adopt only allowances and benefits comparable to those authorized for members of the Foreign Service under the Foreign Service Act of 1980 or other applicable laws. Section 4(b)(1) does not authorize CIA to adopt Agency-unique allowances and benefits such as those authorized under sections 4(b)(2) and (3). Section 4(b)(5), however, still requires that the Intelligence Committees be notified prior to implementation of section 4(b)(1) allowances and benefits. The notification requirement for these section 4(b)(1) regulations adds nearly a month to CIA's process for implementation of employee-friendly policies that enhance morale or meet recruitment and retention concerns—allowances and benefits already authorized for members of the Foreign Service. In order to speed implementation of these section 4(b)(1) allowances and benefits, the Committee amends section 4(b)(5) to exempt section 4(b)(1) implementing regulations from the prior notification requirement.

Section 21(f)(2)(B) of the Central Intelligence Agency Act of 1949

The Committee removes the technically expired requirements of section 21(f)(2)(B) of the CIA Act (50 U.S.C. 403u(f)(2)(B)). This subparagraph required the Director of Central Intelligence to obtain the approval of the Director of OMB and to notify the Intelligence Committees before expending amounts in the CSP Working Capital Fund that are attributable to certain fees imposed and collected under the program. Although CIA has continued to comply with the terms of this expired mandate, the approval and notification requirements set forth in the subparagraph are no longer necessary given CIA experience using CSP authorities. Removing the requirement of subparagraph (f)(2)(b) will not deprive OMB of its oversight role with respect to the CSP. Moreover, the Committee expects that CIA will also continue to comply with other generally applicable requirements for informing Congress of information relating to the management of the CSP, such as the requirements of Title V of the National Security Act of 1947.

INTELLIGENCE COLLECTION, ANALYSIS, AND DISSEMINATION

"Hard Target" Human Intelligence

The invaluable contributions of accurate Human Intelligence (HUMINT) to United States efforts in Operation Enduring Freedom, Operation Iraqi Freedom, and the global war on terrorism are evident.

Particularly in the context of the 107th Congress's Joint Inquiry into the terrorist attacks of September 11, 2001, various Committee Members expressed concern about the need for more vigorous HUMINT collection—especially unilateral collection—under non-official cover and from non-traditional HUMINT "platforms." Some experts have even suggested the need for the creation of a small, highly-specialized semi- or fully-independent HUMINT entity charged with collecting against non-traditional targets and rogue

states that traditionally have proven highly resistant to HUMINT penetration involving traditional official-cover operations.

Without endorsing such a radical solution at this time, the Committee attaches the highest degree of importance to far more aggressive and sustained non-traditional HUMINT collection program. The Intelligence Community must act now to meet the United States requirement for much improved HUMINT collection against hard targets. This will require diligent effort and new approaches to HUMINT management within existing agency components. The Committee hopes and expects that the Director of Central Intelligence will ensure the implementation and success of such changes within the Intelligence Community.

Pilot program on analysis of signals and other intelligence by intelligence analysts of various elements of the Intelligence Community

The Committee has become increasingly concerned in recent years about bureaucratic and cultural obstacles to effective information and data sharing. Such resistance to data access by "outsiders" within the Intelligence Community—let alone to other entities such as analysts at the new Department of Homeland Security—causes at least three serious problems.

First, it impedes the ability of the Intelligence Community to adopt state-of-the-art data-mining and analytical tools that are badly needed to help analysts cope with the flood of information brought in by collection components. Cutting-edge analytical tools, many of which are already in use in the private sector, increasingly involve innovative automated or computer-assisted tools to perform large-scale, multi-database analysis and pattern recognition. Using such approaches within the Intelligence Community, however, cannot proceed far without a significant revision of current orthodoxy as to information "ownership" and control.

Second, barriers to data access inhibit the Intelligence Community's ability to understand, correlate, and assess information that they already possess. Data-control restrictions sometimes impede sharing within an individual element of the Community, as well as between elements, limiting the effectiveness of analytical work far beyond what is necessary to protect highly sensitive information from undue risk of compromise.

Third, barriers to data access prevent the Community from employing other elements' analysts in understanding available information—both for the basic purpose of reducing data overload, and for more sophisticated goals like applying fresh analytical perspectives and experience to existing analytical tasks. The Committee supports additional analytic views to issues, and those views can only be enriched when informed by access to all available information and data.

The NSA, in particular, is an analytical organization that is far too small to handle the volumes of data that it collects. The reluctance of NSA to give other agency analysts access to data that NSA analysts do not have time or priority to review—even when such analysts are as well trained as NSA personnel in protecting "U.S. person" information—has prevented the use of non-NSA analytic manpower to help narrow the gap between collection and analysis and to ensure that more of the unevaluated NSA data is reviewed

by an analyst. It has also drained NSA of trained analysts, because the agency elects to send many of its analysts to other agencies and organizations to supervise and regulate the small degree of NSA information sharing that does occur.

If other agency analysts were properly trained in the rules and procedures governing the handling of SIGINT information (as many are) and these analysts enjoyed the trust of NSA, such analysts would provide "value added" beyond their numbers. Many NSA liaison officers who are now situated in other Intelligence Community agencies to provide those agencies with the ability to access NSA data could return to full-time NSA analytical work.

It has proven difficult to achieve significant improvements in data sharing and information access within and between elements of the United States Intelligence Community. The events of September 11, 2001—and the record of the Community's preparedness for these terrorist atrocities, as detailed by the Senate and House Intelligence Committees' Joint Inquiry during the 107th Congress—make immediate action and cooperation imperative. Accordingly, in Section 314, the Committee requires that concrete steps be taken to pave the way for a future of vastly improved data sharing and information analysis within the Intelligence Community.

Section 314 requires NSA to develop a pilot program to improve the ability of analysts in other Intelligence Community elements to obtain access to and analyze data collected and held by NSA, while retaining appropriate handling safeguards. The pilot program's objectives are: (a) to augment the Intelligence Community's ability to undertake true "all-source fusion" analysis in support of intelligence requirements by helping build a legal and practical foundation for increased inter-agency cooperation and data sharing; (b) to increase to the maximum practicable extent the proportion of NSA-collected information that is reviewed and assessed by intelligence analysts; and (c) to reduce the drain on NSA analytical manpower caused by current barriers to inter-agency information sharing.

Not later than December 31, 2003, therefore, NSA must begin to implement a program to:

a. Develop efficient and effective methods for certifying that designated analysts from other agencies are properly trained in the relevant procedures for handling SIGINT information and for "minimizing" any "U.S. person" information that might be contained therein so that such analysts may be given access to NSA databases in an identical fashion to NSA analysts; those analysts from other agencies will be designated as requiring such access by the head of their parent agency, who will retain full accountability for the analytic products produced by such agency's analysts; and

b. Explore and improve innovative ways to allow other agencies to apply their analytical expertise to NSA data, including the use of "detailees in place" (i.e., other-agency employees who are notionally detailed to NSA, thus becoming part of the SIGINT enterprise while remaining at their home agency).

Pilot program on training for intelligence analysts

Current programs that encourage students to pursue educational programs relevant to national security or foreign language training have not produced the number of qualified analysts or foreign lan-

guage experts necessary to meet the ongoing needs of the Intelligence Community. Although the David L. Boren National Security Education Act of 1991, Title VIII, Public Law 102–183 (Dec. 4, 1991) moves in the right direction, the David L. Boren National Security Education Program (NSEP) places students in national security positions throughout the Federal Government, not merely within the analytic components of the Intelligence Community.

To address the shortage in language proficient and area expert analytic capabilities within the Intelligence Community, the Committee proposes the Director of Central Intelligence establish a ROTC-like Intelligence Analyst Program. This program should seek to increase the number of qualified entry-level intelligence professional analysts available to the Intelligence Community. The goal of the program should be to recruit entry-level analysts and operations specialists with enhanced analytic and foreign language skills who are committed to a career in the Community. The Committee believes this program should be national in scope (conducted at universities throughout the United States), able to identify individuals interested in working in the Intelligence Community, able to provide financial assistance to participants, and capable of providing guidance to participants in selecting courses that would be most useful for an intelligence analyst's career. The program should also include educating participants on the various analytic specialties and opportunities within the Intelligence Community. Prerequisites of the program, and financial assistance thereunder, should include the ability to obtain a security clearance and a commitment for service within the Intelligence Community.

The Committee is pleased that the ADCI/A&P has expressed strong support of the goals of this initiative. Moreover, the Committee believes that the ADCI/A&P is the proper entity to manage such a pilot program for approximately 150 students in fiscal year 2004. Therefore, the Committee recommends an increase of $8.0 million to the ADCI/A&P to create and manage this pilot program.

Report on modifications of policy and law on classified information to facilitate sharing of information for national security purposes

The Committee is concerned that Executive Orders 12333 and 12958 and related regulations and policies may inappropriately limit the effective sharing of intelligence information and data. The Committee therefore has several provisions within the Bill to improve sharing within the Intelligence Community to enhance the quality and timeliness of intelligence products. Furthermore, it is the sense of the Committee that information sharing will become increasingly important as the Department of Homeland Security endeavors to move critical information in both directions between the Intelligence Community and regional, state, and local governments.

Of particular concern to the Committee are various sections in Executive Orders 12333 and 12958 that the Administration should expeditiously review to accurately reflect the movement to electronic data collection and storage and to address the requirement to more effectively assess and share pertinent national security information. The war on terrorism and the proliferation of weapons of mass destruction require foreign and domestic and national and

local partners to effectively collaborate on analysis and coordinate on operations. Achieving this aim will require the U.S. Government to move beyond the paradigm imposed by individual agency "ownership" of information. In that regard, the Committee notes that agencies that collect information often do not have the requisite analytic workforce to fully exploit the data they collect. Further, expanded access to data—providing it is done securely—will foster more rapid access and more competitive analysis and exploitation. Notwithstanding extremely sensitive security, operational, and related matters, the President should continue to encourage broader and more secure exchange of information within the Intelligence Community and between the Community and its many consumers. Executive Order 12958 should be revised not only to remove restrictive impediments within the Executive Order as to the interagency sharing of classified information, but also to facilitate sharing and access (except in narrowly defined circumstances). Executive Order 12333 similarly needs to be revised such that other organizations besides NSA can engage in SIGINT activities, specifically analysis of SIGINT information that has been lawfully collected.

Revisions to Executive Orders 12333 and 12958 are needed, but represent one of many issues that need to be addressed to achieve greater teamwork in the defense of the nation. Technical solutions, such as the need to implement machine-enabled processes to automatically tag data, are needed to facilitate efficient access and analysis. Further, the Intelligence Community must recognize that information sharing cannot succeed without revised security policies and technologies. This Bill, therefore, requires several related reports, including reviews of security clearance procedures, the threats to networks posed by "cleared insiders," and the growing reliance of the United States on foreign hardware and software. Only with a broad approach, encompassing policy and technology and security and sharing, can we achieve the maximum advantages offered by modern information technologies and a highly-trained and motivated workforce.

The Committee requests that the President review Executive Orders 12333 and 12598 and submit a report within 6 months on potential changes to the Executive Orders or legislative actions which could be applied to facilitate information sharing and data access across the Intelligence Community.

Report on data-mining capabilities for the Intelligence Community

Data mining is emerging as potentially one of the most valuable tools for Intelligence Community analysts. Data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. This technology has the potential to provide intelligence analysts with the capability to identify terrorists, to recognize the development and proliferation of weapons of mass destruction, and to detect illicit narcotics activity (e.g., communications, money transfers, and travel) by examining voluminous records.

The Committee is concerned, however, that components of the Intelligence Community are investing in a variety of data-mining capabilities without sufficient coordination of Community-wide data-mining requirements. Strategic planning in this area is vital to en-

sure that there is no redundancy of effort and that interface standards are in place to enable collaboration and cross-program application, as required.

Accordingly, the Committee directs that the Chief Information Officer for the Intelligence Community (CIO) and the ADCI/A&P jointly review data-mining capabilities throughout the Intelligence Community and assess which capabilities meet Intelligence Community analytic requirements. The CIO will publish guidelines to the Community on standards and protocols to enable cross-agency interfaces for migration and data-level information exchange. The results of this assessment should be included in a written report to the House and Senate Intelligence Committees (submitted no later than December 1, 2003) and should include funding requirements for respective data-mining capabilities.

SECURITY AND COUNTERINTELLIGENCE

Although the Committee has sought to eliminate or limit the number of reporting obligations placed on the Intelligence Community, several issues—from security investigations of U.S. Government personnel to the protection of the sensitive national security information maintained by the U.S. Government—require closer examination. To that end, the bill contains a number of one-time reports that will aid the Committee in the careful analysis of the issues presented.

Protecting against unauthorized disclosures of classified information

For some time, the Committee has been greatly concerned about the dangers posed to United States national security from the epidemic of "leaking"—when persons with detailed access to highly sensitive national security information reveal it to unauthorized persons. As President Bush, Secretary of Defense Rumsfeld, Attorney General Ashcroft, Federal Bureau of Intelligence Director Mueller, Director of Central Intelligence Tenet, and many other government officials have repeatedly emphasized, unauthorized disclosures of national security information impose huge and ongoing costs. Such leaks give valuable intelligence to our adversaries, can cost the lives of intelligence sources, imperil foreign government liaison relationships, compromise collection capabilities, imperil the lives of American servicemen and women and the public at large, and greatly impede the U.S. Government ability to protect and advance vital national security interests in the war on terrorism, in fighting foreign espionage, and in prosecuting military campaigns in Iraq and elsewhere. Such leaks also cost the American taxpayer vast sums of money, because capabilities compromised due to leaks must be slowly, laboriously, and expensively rebuilt—or new and costly substitutes must be found.

In the Intelligence Authorization Bill for Fiscal Year 2001, Congress attempted to pass legislation making it a felony to disclose properly classified information. President Clinton vetoed the legislation, however, and the Authorization Act was only made law after Congress had removed the section criminalizing unauthorized disclosures. Understanding that such a broad measure still appears to lack political support—despite the demonstrable costs that today's "leak culture" has imposed, especially since September 11, 2001—

the Committee wishes to encourage the Executive Branch to adopt a new and more aggressive approach to leak issues. The Committee recommends that the U.S. Government consider the workability of aggressive criminal and civil enforcement, even civil compensatory remedies (e.g., liquidated damages).

Coordination of United States Government research on security evaluations

In October 2002, the National Academies of Science released a report entitled, "The Polygraph and Lie Detection"—"a scientific review of the research on polygraph examinations that pertains to their validity and reliability, in particular for personnel security screening." In the report—the first comprehensive assessment of the polygraph since the 1983 study by the U.S. Office of Technology Assessment—the National Academies stated:

> [W]e recommend an expanded research effort directed at methods for deterring and detecting major security threats, including efforts to improve techniques for security screening. * * * We cannot guarantee that research related to techniques for detecting deception will yield valuable practical payoff for national security, even in the long term. However, given the seriousness of the national need, an expanded research effort appears worthwhile. * * * The research program we envision would seek any edge that science can provide for deterring and detecting security threats. It would have two major objectives: (1) to provide Federal agencies with methods of the highest possible scientific validity for protecting national security by deterring and detecting espionage, sabotage, terrorism, and other major security threats; and (2) to make these agencies fully aware of the strengths and limitations of the techniques they use.

In Section 355, the Committee authorizes $500,000 from the Intelligence Community Management Account for the National Science Foundation and the Office of Science and Technology to convene components of the U.S. Government to provide a forum to catalogue and coordinate Federally-funded research activities relating to the development of new techniques in the behavioral, psychological, or physiological assessment of individuals to be used in security evaluations. This effort is intended to serve as an important step in developing a more focused research effort leading to the development of alternatives to the polygraph as a security evaluation tool for the U.S. Government. By March 1, 2004, the National Science Foundation and the Office of Science and Technology are required to jointly submit to Congress a written report identifying the research most likely to advance the understanding of the use of such assessments of individuals in security evaluations; distinguish between short-term and long-term areas of research in order to maximize the utility of short-term and long-term research on such assessments; identify the Federal departments and agencies best suited to support such research; and develop recommendations for coordinating future Federally-funded research for the development, improvement, or enhancement of security evaluations. The components of the Federal Government who will participate in

this effort include DoD, DoE, the Department of State, the Department of Justice, the Department of Homeland Security, the Director of Central Intelligence, the Federal Bureau of Investigation, and the National Counterintelligence Executive.

Report on cleared insider threats to classified computer networks

The Committee is concerned that the classified computer networks of the U.S. Government lack adequate protections from cleared insiders and from certain outside threats. Accordingly, section 331 requires the Director of Central Intelligence, in conjunction with the Secretary of Defense, to provide a one-time report to Congress. The report should assess the national security risks posed by "cleared insiders" that are inherent in current computer security practices within the Intelligence Community and DoD with regard to vulnerabilities such as Information Warfare (IW), Information Operations (IO), Computer Network Exploitation (CNE), and Computer Network Attack (CNA) activity by foreign governments, international terrorist organizations, or organized crime groups. In particular, this report should describe the risks inherent in furnishing to users of local area networks (LANs) and wide-area networks (WANs) that include classified information such capabilities as e-mail, upload/download authorization, and removable storage media without comprehensive firewalls, accountability procedures, or other appropriate security controls. The Committee understands, for instance, that thousands of classified computer terminals within DoD may suffer from these vulnerabilities, which have been highlighted by recent exercises conducted within the U.S. Government in light of the Regan and Hanssen espionage cases. The Committee expects that the report should not only assess what vulnerabilities exist in this regard, but should also describe in detail what steps are being taken to eliminate these threats, including any budget requirements to address shortfalls.

Report on security background investigations and clearance procedures of the United States Government

Most publicly known instances of foreign espionage in this country have been committed by persons who legitimately obtained sensitive security clearances before deciding to betray their country. The Committee is concerned that current security investigations, however, focus more upon screening individuals prior to giving them clearances than upon ascertaining their trustworthiness on an ongoing basis. With this in mind, the Committee has requested a report to assess the relative risks of pre-clearance and post-clearance compromise. This report should state whether current approaches address adequately the risk of cleared employees compromising classified information after their period of access to such information has already begun. The report should also make recommendations about how background investigations might in the future be better targeted to historically verifiable counterintelligence vulnerabilities.

Report on United States dependence on computer hardware and software manufactured overseas

After 1973, when the risks inherent in America's reliance on foreign oil became clear, many positive steps were taken to ameliorate

United States vulnerabilities. Those steps included, among other things, establishment of a strategic petroleum reserve, establishment of a Central Command, and research and development into alternative fuel supplies. In many respects, information technology has become as important to the functioning of the United States economy as oil, and the growing dependence of the United States on foreign information technology raises concerns similar to those raised with respect to foreign oil dependence. Unlike foreign oil dependence, however, United States dependence on foreign information technology creates opportunities for espionage and clandestine information operations that are extremely difficult to detect. In that regard, the Committee notes that most of the leading suppliers of hardware and software to the United States are countries that the Federal Bureau of Investigation indicates are already actively engaged in economic espionage against this country.

To accurately determine the dimensions of the problem relating to United States dependence on foreign hardware and software, the Committee directs the Director of Central Intelligence to prepare a thorough evaluation of the trends within this critical industry and the strategic implications of increasing United States reliance on foreign hardware and software. Recognizing that some of the greatest sources of expertise on this issue reside in the private sector, the Committee authorizes and supports such consultation with industry as may be required. Once the Committee has received this analysis, Congress will be in a better a position to develop appropriate policies to mitigate this new vulnerability.

SUMMARY OF REPORTING REQUIREMENTS

One-time reporting requirements

The Fiscal Year 2004 Intelligence Authorization Bill requires the following one-time reporting requirements, which are discussed throughout the report:

(a) Report on cleared insider threat to classified computer networks;

(b) Report on security background investigations and security clearance procedures of the United States Government;

(c) Report on detail of civilian intelligence personnel among elements of the Intelligence Community and the Department of Defense;

(d) Report on modifications of policy and law on classified information to facilitate to sharing of information for national security purposes;

(e) Report of Secretary of Defense and Director of Central Intelligence on strategic planning;

(f) Report on United States dependence of computer hardware and software manufactured overseas;

(g) Report on intelligence lessons learned from military operations in Iraq;

(h) Report on conventional weapons and ammunition obtained by Iraq in violation of certain United Nations Security Council resolutions;

(i) Report on data-mining capabilities for the Intelligence Community;

(j) Report on the National Security Agency Senior Acquisition Executive;

(k) Quarterly report baselining all program, projects, and activities ongoing within the Consolidated Cryptologic Program;

(l) Report on a review of the "Public Private Partnership" and the "Private Financing Initiative" concepts for application to Menwith Hill Station.

Reports repealed or cancelled

The following is a list of reports that are repealed or cancelled, and are no longer required to be submitted to the Committee. Additional reports repealed in the Fiscal Year 2004 Intelligence Authorization Bill are contained in the Classified Annex.

(a) Annual Evaluation of Performance and Responsiveness of Intelligence Community;

(b) Periodic and Special Reports on Disclosure of Intelligence Information to the United Nations;

(c) Annual Report on Intelligence Community Cooperation with Counterdrug Activities;

(d) Annual Report on Russian Nuclear Facilities;

(e) Annual Report on Covert Leases;

(f) Annual Report on Protection of Covert Agents;

(g) Annual Report on Certain Foreign Companies Involved in Proliferation of Weapons of Mass Destruction;

(h) Annual Report on Intelligence Activities of People's Republic of China;

(i) Annual Report on Coordination of Counterintelligence Matters with the Federal Bureau of Investigation;

(j) Reports on Decisions not to Prosecute Violations of Classified Information Procedures Act;

(k) Report on Postemployment Assistance for Terminated Intelligence Employees;

(l) Annual Report on Activities of Federal Bureau of Investigation Personnel Outside the United States;

(m) Annual Report on Exceptions to Consumer Disclosure Requirements for National Security Investigations;

(n) Recurring report(s) on comprehensive annual reviews of customer satisfaction;

(o) Recurring report on the Intelligence Community's information infrastructure.

COMMITTEE ACTION

On May 1, 2003, the Select Committee on Intelligence approved the Bill and ordered that it be favorably reported.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a) of rule XXVI of the Standing Rules of the Senate, the estimated costs incurred in carrying out the provisions of this Bill for fiscal year 2003 are set forth in the Classified Annex to this Bill. Estimates of the costs incurred in carrying out this Bill in the five fiscal years thereafter are not available from the Executive Branch, and therefore the Committee deems it impractical, pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, to include such estimates in this report. On [ ], 2003, the Committee transmitted this Bill to the

Congressional Budget Office and requested that it conduct an estimate of the costs incurred in carrying out the provisions of this Bill.

EVALUATION OF REGULATORY IMPACT

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

CHANGES IN EXISTING LAW

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.

○