AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

105TH CONGRESS, 2d Session | 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

MAY 7, 1998.—Ordered to be printed

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

REPORT

[To accompany S. 2052]

The Select Committee on Intelligence, having considered the original bill (S. 2052), which authorizes appropriations for fiscal year 1999 for intelligence-related activities and programs of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and which accomplishes other purposes, reports favorably thereon and recommends that the bill pass.

PURPOSE OF THE BILL

This bill will:

(1) Authorize appropriations for fiscal year 1999 for (a) the intelligence activities and programs of the United States Government; (b) the Central Intelligence Agency Retirement and Disability System; and (c) the Community Management Account of the Director of Central Intelligence;

(2) Authorize the personnel ceilings as of September 30, 1999, for intelligence activities of the United States Government and for the Community Management Account of the Director of Central Intelligence;

(3) Authorize the Director of Central Intelligence, with Office of Management and Budget approval, to exceed the personnel ceilings by up to two percent;

(4) Extend for one additional year the President's authority to delay the imposition of proliferation-related sanctions when necessary to protect an intelligence source or method or an ongoing criminal investigation;

59–010

(5) Extend for two additional years the Secretary of Defense's authority to engage in commercial activities as security for intelligence collection activities;

(6) Amend the National Security Education Act of 1991 to include the study of counter-proliferation within the scope of the Act;

(7) Extend for two additional years the Director of Central Intelligence's authority under the Central Intelligence Agency Voluntary Separation Pay Act of 1993 to offer separation pay to employees;

(8) Authorize the Director of Central Intelligence to designate personnel to carry firearms to protect current and former Agency personnel and their immediate families;

(9) Authorize the Central Intelligence Agency's Inspector General to review and comment in the Inspector General's semiannual reports on existing and proposed legislation relating to programs and operations of the Agency;

(10) Authorize the Attorney General or a designated attorney for the Government to apply for a court order authorizing the installation and use of a pen register or trap and trace device for an investigation to gather foreign intelligence information or information concerning international terrorism;

(11) Authorize the Director of the Federal Bureau of Investigation or a designee to apply for a court order to require common carriers, public accommodation facilities, or vehicle rental facilities to release certain records in their possession relating to a foreign intelligence or international terrorism investigation; and

(12) Ensure that employees within the Intelligence Community are made aware that they may, without prior authorization, disclose certain information to Congress, including classified information, that they reasonably believe is specific and direct evidence of—a violation of law, rule or regulation; a false statement to Congress on an issue of material fact; or gross mismanagement, a gross waste of funds, a flagrant abuse of authority, or a substantial and specific danger to public health or safety.

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. The classified annex has the same status as any Senate Report, and the Committee fully expects the Intelligence Community to comply with the limitations, guidelines, directions, and recommendations contained therein.

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 and to the President. The President shall provide for appropriate distribution within the Executive Branch.

SCOPE OF COMMITTEE REVIEW

The Committee conducted a detailed review of the fiscal year 1999 budget requests for the National Foreign Intelligence Program (NFIP) of the Director of Central Intelligence; the Joint Military Intelligence Program (JMIP) of the Deputy Secretary of Defense; and the Tactical Intelligence and Related Activities (TIARA) of the military services. The Committee's review entailed a series of briefings and hearings with senior intelligence officials, numerous staff briefings, review of budget justification materials, and numerous written responses provided by the Intelligence Community to specific questions posed by the Committee. The Committee also monitors compliance with numerous reporting requirements contained in statute. Each report is scrutinized by the Committee and appropriate action is taken when necessary.

In accordance with a Memorandum of Agreement with the Senate Armed Services Committee (SASC), the Committee is including its recommendations on both JMIP and TIARA in its public report and classified annex. The Senate Select Committee on Intelligence (SSCI) has agreed that JMIP and TIARA issues will continue to be authorized in the defense authorization bill. The SASC has also agreed to involve the SSCI staff in staff-level defense authorization conference meetings and to provide the Chairman and Vice Chairman of the SSCI the opportunity to consult with the SASC Chairman and Ranking Member before a JMIP or TIARA issue is finally closed out in conference in a manner with which they disagree. The Committee looks forward to continuing its productive relationship with the SASC on all issues of mutual concern.

In addition to its annual review of the Administration's budget request, the Committee performs continuing oversight of various intelligence activities and programs. The Committee has a dedicated audit staff that conducts indepth audits and reviews of specific programs and activities identified by the Committee as needing a thorough and concentrated scrutiny. For example, the Committee audit staff recently concluded examinations of the use of cover by the Central Intelligence Agency and the administration of the Foreign Intelligence Surveillance Act of 1978. These inquiries frequently lead to Committee action with respect to the authorities, applicable laws, and budget of the activity or program concerned.

The Committee also established a Technical Advisory Group (TAG) in 1997. The TAG is an independent panel of twenty-two experts drawn from the private sector. Each member of the TAG was selected by the Committee for their extensive expertise in a particular discipline. The purpose of the TAG is to provide the Committee an objective and comprehensive evaluation of various intelligence programs and activities. Many of the TAG members have never worked within the Intelligence Community and therefore

being a fresh and independent perspective to intelligence programs and activities. The results of these examinations and the TAG will be discussed later in its report.

COMMITTEE RECOMMENDATIONS

The vast majority of the Committee's specific recommendations relating to the Administration's budget request for intelligence and intelligence-related activities are classified and are contained in the classified schedule of authorizations and the classified annex. The Committee is committed, however, to making its concerns and priorities for intelligence programs and activities public to the greatest extent possible consistent with the nation's security. Therefore, the Committee has included in this report information that is unclassified and available to the public.

NATIONAL FOREIGN INTELLIGENCE PROGRAM

Areas of committee emphasis

The Committee has continued its bipartisan efforts to "right-size" and "re-tool" U.S. Intelligence Community programs and activities to reflect the new, post-Cold War era threats and challenges to U.S. national security.

Specifically, the Committee recommends important new investments and initiatives in high-priority areas. These include: aggressive efforts in what the committee chairman has called the "five C's" (counter-proliferation, counter-narcotics, counter-terrorism, counter-intelligence, and covert action); bolstering advanced research and development across the Intelligence Community to maintain the U.S. technological edge; improving the skills and tools of clandestine service personnel; developing new and innovative approaches to understanding "hard target" countries; building up capabilities in the area of measurments and signatures intelligence; and enhancing analytical capabilities as well as tools for conducting information operations.

The Commission recommends significant funding increases in each of the priority areas listed above. At the same time, however, the Committee recommends reductions in programs and activities that are lower-priority or poorly justified, redundant, or that cannot be executed. Details of the Committee's recommendations are included in the Classified Annex accompanying this report.

Department of Defense Foreign Counterintelligence Program (DoD FCIP)

The Committee notes the precipitous decrease in personnel and funding requested for the DoD FCIP since fiscal year 1993. The resources dedicated to the military's counterintelligence mission have decreased by nearly one half in five years. This significant decline, however, has been accompanied by a marked increase in operational tempo and increased emphasis on force protection which draws heavily on counterintelligence resources.

As Congress strives to achieve and maintain a balanced budget, the Committee recognizes the need to reduce spending in many areas. The Committee is concerned, however, that certain programs and activities within the DoD FCIP have been cut without a realis-

tic evaluation of the impact on the Department's counterintelligence mission. It appears to the Committee that the concept of doing more with less has led to declining morale, lack of training, and attrition of personnel with a corresponding loss of expertise. Further, the decreases in FCIP funding belie the growing dependence by commanders in the field on information collected by counterintelligence personnel. A 1996 Director of Central Intelligence study estimated that nearly 70% of the information used by combatant commanders for force protection comes from counterintelligence and HUMINT personnel. If this is indeed the case, the Committee would expect the counterintelligence mission to be targeted for funding increases to strengthen our collection capabilities and enhance our analytical capability in the field.

Therefore, the Secretary of Defense shall submit, by March 15, 1999, a report to the Congressional Intelligence Committee comparing the decrease in DoD FCIP, service TIARA, and Security and Intelligence Activities funding over the last five years with the operational demands placed on the Department's counterintelligence forces. The comparison shall address the average deployment schedule of counterintelligence personnel for each of the past five years. The report shall also explain the analytical methodology used by the Department to conduct mission impact analysis before it mandates cuts to the counterintelligence force structure. If such an analysis is conducted, the report shall include the Department's mission impact conclusions for the past five years. If no impact analysis is conducted, the report shall explain why no such analysis is conducted. The report shall also determine the optimum counterintelligence force structure considering intelligence requirements, operational tempo, and increased emphasis on force protection over the last five years.

Federal Bureau of Investigation foreign counterintelligence

The Committee's audit staff recently completed a comprehensive review of the implementation and administration of the Foreign Intelligence Surveillance Act of 1978. During the course of this examination, the audit staff encountered many instances where the FBI has failed to address technological challenges that may, in time, degrade the Bureau's ability to collected critical counterintelligence and counter-terrorism information. Further, the audit revealed a Bureau-wide deficiency in information systems modernization and implementation. The dearth and diversity of information systems technology throughout the National Security Division, in particular, suggests that the Bureau has yet to develop a unified and comprehensive plan to address this challenge. The Committee believe that the Bureau either has neglected an opportunity to maximize the efficiencies available through automation, or lack the requisite resources, expertise and vision to develop, install, and operate Bureau-wide systems.

The Committee understands that a Strategic Management Task Force within the Bureau is conducting a comprehensive review of the use of collection and information systems technology throughout the FBI. While this effort is long overdue, the Committee is encouraged by this initiative. The Committee urges the Director to share the findings and recommendations of this review with the

Congressional Intelligence Committees. The Committee is concerned that the ability to conduct electronic surveillance may fall prey to the advance of technology if the Bureau does not keep pace with new software and hardware developments. Additionally, the Committee wishes to emphasize the need for systems that link elements within the National Security Division so that counterintelligence and counter-terrorism information may be disseminated, shared, and accessed simultaneously by agents, language specialists, and analysts.

National Drug Intelligence Center

As the Managers indicated in the Conference Report accompanying S. 858, the Intelligence Authorization Act for Fiscal Year 1998, the continued funding of the National Drug Intelligence Center (NDIC) from the National Foreign Intelligence Program deserves study. The Committee is prepared to support and provide additional resources for meritorious initiatives generated by the NDIC to the extent that the NDIC is truly an element of the Intelligence Community. The Committee cannot evaluate such initiatives, however, until it receives the report mandated in last year's Act. Congress urged the President to carefully examine the operations of the NDIC and report to the Congressional Intelligence Committees before April 1, 1998. Additionally, the managers directed that this examination should be undertaken and reported as a part of the National Counter-Narcotics Architecture Review being prepared by the Office of National Drug Control Policy (ONDCP). To date, no report has been received.

Despite numerous attempts to obtain this information from the ONDCP, no information has been made available to support accurate and responsible budgeting of NDIC activities. The mandated report required detailed information on current and proposed efforts to structure the NDIC to effectively coordinate and consolidate strategic drug intelligence from national security and law enforcement agencies. It also required a detailed description of those steps that have been taken to ensure that the relevant national security and law enforcement agencies are providing the NDIC with access to data needed to accomplish this task.

The Manager's also agreed that upon receipt of this report, the Committees would reconsider whether it is appropriate to continue funding the NDIC as a part of the National Foreign Intelligence Program.

Therefore, because the report has not yet been received, the transfer of funds described in Section 104(e)(2), shall not be undertaken until 30 days after the Congressional Intelligence Committees are in receipt of the report mandated in the Intelligence Authorization Act for Fiscal Year 1998.

Money laundering activity by foreign narcotics traffickers

The Committee is concerned by the number and magnitude of illicit financial transactions that take place within American financial systems initiated by foreign narcotics trafficking organizations. The Committee has received several briefings and reports from various government agencies, conducted hearings on this and related

issues, and understands that the magnitude of the problem may exceed several hundred billion dollars annually.

The Committee has concluded that there is not enough emphasis being placed on combating this serious problem. Accordingly, the Committee has augmented the resources of the DCI's Crime and Narcotics Center to begin to address this shortfall. It is also the Committee's intention to investigate this area further and consider, when appropriate, legislative initiatives.

Central Services Program Working Capital Fund (CSPWCF)

The Committee strongly supports the Central Intelligence Agency's Directorate of Administration (DA) as it continues to make steady progress in its initiative—begun in fiscal year 1998—to put administrative service providers on a business-like footing through use of the CSPWCF. The Logistics Operation Center (LOC) was the first business area shifted into the CSP.

The budget request did not include funds for CSPWCF because the DA continues to refine estimates of the funds required to shift six additional business areas—transportation services, facilities management and maintenance, foreign field communications, applications development, training, and telephone services—into CSPWCF in fiscal year 1999. By the end of fiscal year 1998, however, the DA will be able to determine the exact amount of funds needed for the CSPWCF in fiscal year 1999 and will address funding as a fiscal year 1999 issue. Once those estimates are known, the Committee urges the Director of Central Intelligence to adequately fund any CSPWCF needs.

Commercial imagery

Since 1993, the Committee has advocated the acquisition and use of commercial imagery where practicable. The Committee has urged the Department of Defense and the Intelligence Community to more aggressively pursue the use of commercial imagery.

Through numerous briefings with the National Imagery and Mapping Agency, the National Reconnaissance Office, and industry representatives, the Committee is convinced that commercial imagery can satisfy a significant quantity of U.S. medium resolution imagery requirements. Current private sector launch plans will provide possibly up to six U.S.-owned satellites that can provide imagery with resolution of one meter prior to the launch of the first satellite in a follow-on, government operated satellite imagery constellation. Unfortunately, NIMA has yet to solicit private sector proposals for acquisition of medium resolution imagery, nor has NIMA evaluated the potential purchase of a commercial satellite to meet future U.S. needs for medium resolution imagery.

In an effort to implement increased use of domestic commercial imagery, the Committee recommends that the Senate Armed Services Committee adopt a "buy America" legislative provision related to acquisition of commercial imagery and further recommends an additional $10.0 million authorization for appropriations for purchase of commercial imagery.

Imagery archiving

The Committee is concerned that the Intelligence Community and Defense have not adequately addressed the preservation of space and airborne reconnaissance imagery. While much of the current value of the investment in imagery reflects national defense requirements, the future value cannot adequately be estimated. The Committee recognizes that the life expectancy of archived imagery is dependent on the media on which it is stored and that some types of media may not survive for long-term use. Therefore the Committee directs the Director of Central Intelligence and Deputy Secretary of Defense to conduct a review of archiving and preservation practices for imagery collected from space and airborne platforms, and deliver to the Committee, not later than March 15, 1999, a report on current and future plans to maintain those archives indefinitely at the lowest cost. The report should also address the architecture for accessing the imagery digitally in a geospatial reference frame. If the study projects a reduction in imagery holdings, the rationale for such reduction shall be explained. Finally, the Committee directs the Director, National Imagery and Mapping Agency, to investigate new data storage technologies to determine whether their application will decrease archival costs by allowing, among other things, higher density storage, longer term storage between restorations, or less stringent storage-environment requirements, while maintaining data quality.

Intelligence dissemination architecture

The Committee notes the progress being made by the Department of Defense in developing a coherent, near-real time intelligence data dissemination architecture. Plans being developed for the Integrated Broadcast System (IBS) will serve as a focal point for continued progress in this regard. The Navy, as Executive Agent for IBS, is to be commended for moving quickly to get the initial broadcast service platform in space. There remains, however, an area of some concern with respect to the overall dissemination architecture relating to the specific bandwidths being acquired within the National Foreign Intelligence Program to support specific broadcast needs that do not seem to have any validated linkage to the IBS program.

The Committee is aware that the Tactical Related Applications (TRAP) Data Dissemination system (TDDS) will provide multiple channels for rapid broadcast of critical intelligence information in support of tactical operations. The distribution center for TDDS is called Upgraded Dissemination Ground Segment (UDGS) and will become operational in fiscal year 1999. This is a very capable system with capacity that is global in scope and flexible in format. This bandwidth must be factored into the IBS architecture and managed as part of that architecture.

Therefore the Committee directs that the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, with the Executive Agent for IBS and the Acquisition Agent for IBS, prepare a study that shows the integration of broadcast systems into the IBS program. This study should validate the location of the UDGS as optimum for the IBS program and give detailed descriptions of the various intelligence source inputs, as well as the

information management scheme that will be implemented to ensure the military customer is getting the necessary information in a usable format. Specifically, the Committee seeks to ensure that the adjudication and deconfliction authorities are adequate to maintain broadcast discipline and ensure that the customer identifies and receives critical intelligence information, as defined by the customer, in a timely manner.

The Committee does not believe that a robust architecture implies a single dissemination system. The Committee is concerned that broadcast services are being buried within intelligence "stovepipes", when they could better serve the same customers in a more efficient and effective manner if they were brought under centralized control within the Department of Defense. This issue has languished in the Department for several years and acquisition decisions have been effected that are not consistent with a "system of systems" approach. The report directed above shall be due not later than March 15, 1999.

NSA declassification

The National Security Agency has several declassification programs, which are split among many offices, and funding for which is buried in the budget submissions of those offices. NSA was unable to provide the Committee with the total amount requested for all declassification programs in fiscal year 1999. In addition, with respect to the only declassification program specifically identified in the Congressional Budget Justification Book, NSA was unable to explain how those resources would be allocated. It is impossible for the Committee to determine the scale of the declassification effort, the effectiveness of declassification tools, and how well NSA is meeting declassification requirements. To enhance oversight, the Committee directs the Director of NSA to consolidate all declassification programs into a single budget submission beginning in fiscal year 2000, to include a breakdown of how the resources will be allocated.

JOINT MILITARY INTELLIGENCE PROGRAM

Joint SIGINT Avionics Family

The objective of Joint SIGINT Avionics (JSAF) is the creation of functional commonality and interoperability among all U.S. airborne reconnaissance platforms, regardless of service or airframe type. Commonality and interoperability are accomplished through an open architecture, common sensor payload, and software reconfigurable processors. The development is being accomplished through a series of technology modules that can be incrementally integrated into existing systems and platforms.

The JSAF is designed to adapt to rapidly changing future threat capabilities through software exploitation rather than by more costly hardware alterations and upgrades. The program is divided into a low band subsystem (LBSS) and a high band subsystem (HBSS). The system design relies on commercial off-the-shelf software and hardware to increase affordability. Initial system implementation is planned for completion in fiscal year 2007.

Currently, there are four platforms scheduled to receive either the LBSS, the HBSS, or both. The Air force plans to install JSAF on two platforms, the RC–135 Rivet Joint and the Air Force special platform. There are 16 of each of the two platforms in the Air Force. The navy plans to install JSAF on its EP–3E aircraft. The Navy maintains 12 EP–3E platforms. The Army plans to install JSAF on nine Airborne Reconnaissance Low (ARL) aircraft for a total of 53 manned platforms. Under the present plan, the Air Force special platform will be the only aircraft equipped with the LBSS and the HBSS.

The LBSS/HBSS production schedule (including development units) is as follows:

	Fiscal years—							
	2000	2001	2002	2003	2004	2005	2006	2007
LBSS	[1] 3	9	10	10	9	7	4	1
HBSS	[1] 1	3	3	3	3	3	1	.....

[1] Developmental units.

In an effort to expedite delivery of this capability, the Committee reviewed as accelerated production effort that would not increase program risk. The Committee found that the delivery schedule could be accelerated by up to three years in the case of the Air Force special platform, and two years with other platforms, by requiring that platforms be equipped with JSAF components at their next depot maintenance (PDM).

Under the current plan, both low and high band subsystems begin delivery to the services in fiscal year 2001 and conclude delivery in fiscal year 2007. During this period, some aircraft will go through a PDM cycle and not have the new component installed even though the components could be readily available. Maintaining these older systems when they could be replaced will increase support costs. An accelerated delivery schedule consistent with platform PDM schedules would be as follows:

	Fiscal years—					
	2000	2001	2002	2003	2004	2005
LBSS	[1] 3	10	14	14	7	5
HBSS	[1] 1	4	.....	6	.....	6

[1] Developmental units.

The accelerated schedule does not increase risk and has no budgetary impact in fiscal year 1999. It requires that funding be accelerated in fiscal years 2000 through 2003 over current plans. The accelerated schedule not only delivers capability faster, but also saves $44 million in initial JSAF costs over the current acquisition plan. The alternative funding profile would be as follows:

[In millions of dollars]

	Prior yrs.	Fiscal years—					TC	Total
		2000	2001	2002	2003	2004		
Baseline	34.6	24.1	192.0	173.5	164.1	105.4	152.4	846.1
Acclerated	34.6	29.7	212.1	238.4	218.5	42.9	25.9	802.1

[In millions of dollars]

	Prior yrs.	Fiscal years—					TC	Total
		2000	2001	2002	2003	2004		
Delta	0	+5.6	+20.1	+64.9	+54.4	−62.5	−126.5	−44.0

The Committee recommends the adoption of language directing the Department of Defense to adopt an accelerated JSAF acquisition strategy consistent with the earliest platform availability for PDM schedules.

Defense Airborne Reconnaissance Program integration & support

The budget request included $17.04 million, an increase of more than 100 percent over fiscal year 1998, for program integration and support. The budget justification materials did not demonstrate a convincing requirement for such a dramatic increase. One of the stated justifications for these funds is development of transfer plans of Unmanned Aerial Vehicle (UAV) capabilities to the services. Given the serious delays in both the High Altitude Endurance UAV and Tactical UAV programs, coupled with the Air Force's negative experience with the Predator program and the fact that the Air Force has conducted detailed planning for assumption of responsibility for the High Altitude Endurance UAV program, the Committee finds the administration's rationale redundant.

Therefore, the Committee recommends a reduction of $8.0 million for Defense Airborne Reconnaissance Program Integration and Support for fiscal year 1999.

Common ground segment

The Committee remains concerned about the delays in the High Altitude Endurance Unmanned Aerial Vehicle (HAE UAV) Advanced Concept Technology Demonstration (ACTD), especially with regard to the Dark Star UAV, which continues to fall further behind schedule. Information provided to the Committee casts serious doubt on the viability of the Dark Star portion of the ACTD.

Because of repeated schedule delays and program problems the Committee believes that the administration request for fiscal year 1999 for the Common Ground Segment cannot be executed in an efficient manner. Therefore, the Committee recommends a reduction of $8.0 million in Common Ground Segment for fiscal year 1999.

Dark Star

Dark Star is the Low Observation air vehicle component in the HAE UAV Advanced Concept Technology Demonstration (ACTD) currently managed by the Defense Advanced Research Projects Agency (DARPA). The Dark Star program remains plagued by program delays and is substantially behind the projected schedule. The Congress has appropriated more than $100.0 million for fiscal years 1997 and 1998 combined, and the administration has requested $40.5 million for fiscal year 1999.

The Committee believes that the unexpended prior year funds and a reduced fiscal year 1999 authorization for appropriations will be sufficient to sustain the Dark Star ACTD through the upcoming

fiscal year. Therefore, the Committee recommends a reduction of $10.0 million for Dark Star in fiscal year 1999.

Interferometric synthetic aperture radar

Forward deployed U.S. armed forces have a need for up-to-date and highly accurate maps that provide three-dimensional location of targets, including altitude, latitude and longitude, and for reconstruction of terrain in a three-dimensional setting for planning combat missions. Airborne interferometric synthetic aperture radar (IFSAR) has the potential to provide such maps with an accuracy and timeliness that meets the demanding digital terrain elevation data (DTED) Level 5 specifications. Such performance would meet all validated Army and Air Force requirements for battlefield visualization and precision strike. A demonstration IFSAR at somewhat lower performance parameters flew successfully on a commercial jet in support of U.S. forces in Bosnia. The Committee believes that this capability can now be transferred to an operational military platform.

Therefore, the Committee recommends an addition of $4.0 million within the Advanced Topographic Mapping System (ATOMS) program for fiscal year 1999 to expedite development of a DTED Level 5 IFSAR for installation on the Army's Airborne Reconnaissance Low (ARL) platform.

IMPROVING INTELLIGENCE COMMUNITY MANAGEMENT AND OPERATION

The biological and chemical weapons threat

In March and April 1998, the Committee held a series of joint hearings with the Judiciary Subcommittee on Technology, Terrorism & Government Information to receive both open and classified testimony on the subject of the biological and chemical threats to the United States by states and non-state actors such as terrorists, and on the United States government's strategy and capabilities to prevent or respond to such an attack. Witnesses included the Attorney General, the Director of the FBI, senior intelligence community officials, medical experts from the U.S. Army and the Centers for Disease Control, and expert private witnesses. In addition, Committee staff met with and debriefed a defector who until 1992 served as a senior scientist in the Soviet/Russian offensive biological weapons program.

In the wake of the 1993 World Trade Center bombing, the 1995 Aum Shinrikyo attack in the Tokyo subway, and most recently, the arrests in Las Vegas of persons suspected of possessing deadly anthrax agent, the Committee has been concerned by the proliferation of biological and chemical weapons and the growing prospect of a terrorist attack against the United States using biological or chemical agents. The Committee has initiated or supported a number of programs to enhance the Intelligence Community's capabilities to monitor this threat, including new legislative authorities in the Intelligence Authorization Act of Fiscal Year 1999 to collect certain kinds of critical preliminary information of relevance to FBI investigations into international terrorism, and to provide policymakers with the information and tools needed to support U.S. counter-proliferation and counter-terrorism policies. The Classified Annex to

the Intelligence Authorization Act for Fiscal Year 1999 continues the Committee's efforts in this regard.

The threat of biological or chemical attack poses extraordinary and, in some cases, unique challenges, ranging from the difficulty of detecting the production of such agents and providing timely warning of a potential attack, to the consequences of a biological event, which could under certain circumstances be more lethal than a nuclear explosion. Of particular concern, from the Committee's viewpoint, are the ready availability and dual use nature of the materials and equipment used to prepare biological and chemical agents; the relative ease with which a small group of terrorists could produce such substances (compared, for example, with nuclear weapons); the possibility of genetic engineering to defeat countermeasures and increase the virulence and infectivity of biological agents; the threats posed by the Iraqi and Iranian biological weapons programs; and concerns over Russia's remaining offensive biological warfare program, which according to published reports could include biological warheads on ICBMs, as well as the potential for transfer of scientific expertise, or actual biological agents, from the Russian program to rogue states or terrorist groups.

Many of the challenges cited above are intrinsic to the nature of biological and chemical weapons, or otherwise largely beyond the capacity of the U.S. Government to influence. The Committee is disturbed, however, by public reports that a major interagency study has revealed widespread problems and deficiencies in the U.S. Government's counter-terrorism strategy and capabilities, including intelligence programs and activities under the Committee's jurisdiction. This is discussed in greater detail in the Classified Annex, where the Committee is directing that the Director of Central Intelligence and the Attorney General report to the Committee on measures they are taking or intend to take to address any shortcomings they have identified.

DoD IG oversight of intelligence issues

In 1995, responding to Congressional concerns about DoD IG oversight of DoD organizations within the Intelligence Community, the DoD IG established an Office of Intelligence Review. The Office of Intelligence Review's mission includes overseeing DoD intelligence programs and activities as well as coordinating activities of the Inspectors General within DoD intelligence agencies such as NSA, NRO, and DIA. Many products of the Office of Intelligence Review have been very useful to this Committee.

In January 1998, as a result of overall DoD IG downsizing, the Office of Intelligence Review was made a separate entity reporting directly to the DoD IG. However, as part of this reorganization, the staffing of the Office of Intelligence Review was cut nearly in half. While the Committee applauds the increased oversight potential created by establishing a separate DoD IG office dedicated to reviewing intelligence programs and activities, it is concerned that current DoD IG resource constraints could result in the Office of Intelligence Review being reduced to an ineffective level or eliminated completely. Over the next fiscal year the Committee will be evaluating the Office of Intelligence Review's ability to continue to provide quality products at its current staffing level.

Computer-proliferation education and training

The United States faces a qualitatively new proliferation challenge to its national security interests. Because the proliferation of weapons of mass destruction (WMD) and their delivery systems poses a paramount, long term threat to the country, the Committee is of the view that the country should utilize education as an essential tool in support of the training of counter-proliferation specialists equipped to address this threat.

At the present time, however, explicit program authority is not available to train American students adequately to confront the proliferation challenge. Particularly noticeable by its absence is government support for graduate training in the counter-proliferation area, which includes WMD technologies and capabilities, missile and other delivery system technologies and capabilities, existing and required domestic response capabilities, motivations and techniques of state and subnational proliferators, and a careful assessment of existing counter-proliferation regimes.

The National Security Education Act (NSEA) was enacted in 1991 "to provide the necessary resources, accountability, and flexibility to meet the national security education needs of the United States, especially as such needs change over time". As drafted in 1991, the NSEA emphasized language and area studies. Since then, the national security needs of the country have changed. In an effort to generate limited but sustained Federal support for counter-proliferation activities and studies, the Committee amends the National Security Education Act of 1991 to (1) specify counter-proliferation studies as a primary area for Federal support, and (2) require that the National Security Education Board established by the Act include the Secretary of Energy. The Committee has as a goal the allocation of not less than one-third of the amounts specified under the Act for the awarding of fellowships to graduate students and grants to institutions of higher learning in the field of counter-proliferation training and studies.

In addressing the threats posed by the proliferation of weapons of mass destruction, the Committee has not only been supportive of the funding requests of the Intelligence Community in combating this threat, but has also pointed the way toward enhanced efforts by the community in newer, nontraditional areas. Committee support for funding of counter-proliferation education and training through an amended National Security Education Act is not only consistent with these efforts but can ultimately contribute to their success.

IMPACT OF TECHNOLOGY ON THE INTELLIGENCE COMMUNITY

Technical Advisory Group

In 1997, the Committee established a Technical Advisory Group (TAG) to consider selected, highly significant technical issues relating to national security or intelligence. The TAG is comprised of leading U.S. scientists and experts in technology and intelligence. The Committee wishes to thank the TAG members for the many hours they devoted to examining both the HUMINT and SIGINT capabilities of the Intelligence Community (IC). The TAG concluded that intelligence collection will pay an increasingly important role

in defending U.S. national security interests, and recommended that the IC develop a comprehensive plan for transition to the future which recognizes the technically sophisticated, rapidly changing world that now confronts the IC. The Committee will continue to review the recommendations of this distinguished group and work with the Director of Central Intelligence to implement them. Many of the initial recommendations of the TAG have been incorporated throughout the Intelligence Authorization Act of 1999.

Encryption

The Committee remains concerned about efforts to inappropriately ease or remove export restrictions on hardware and software encryption products. Export controls on encryption and other products serve a clearly defined purpose—to protect our nation's security. Therefore, the Committee believes that the effects on U.S. national security must be the paramount concern when considering any proposed change to encryption export policy, and will seek referral of any legislation regarding encryption export policy under its jurisdiction established under Senate Resolution 400.

Export restrictions on encryption products assist the Intelligence Community in its signals intelligence mission. By collecting and analyzing signals intelligence, U.S. intelligence agencies seek to understand the policies, intentions, and plans of foreign state and nonstate actors. Signals intelligence plays an important role in the formation of American foreign and defense policy. It is also a significant factor in U.S. efforts to protect its citizens and soldiers against terrorism, the proliferation of weapons of mass destruction, narcotics trafficking, international crime and other threats to our nation's security.

While the Committee recognizes the commercial interest in easing or removing export restrictions, it believes the safety of our citizens and soldiers should be the predominant concern when considering U.S. policy towards the export of any product. The Committee supports the continued control of encryption products, and believes that a comprehensive strategy on encryption export policy can and must be developed that addresses national security concerns as well as the promotion of American commercial interests abroad. The Committee looks forward to working with senior Administration officials in developing such a strategy.

Intelligence Community role in national infrastructure protection

The Committee believes the Intelligence Community has an important role to play in the protection of our nation's critical infrastructure. The President's Commission on Critical Infrastructure Protection (PCCIP) issued a report in October 1997 which identified five critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—that are essential to national defense, public safety, economic prosperity, and quality of life. In pursuit of greater effectiveness and efficiency, the private and public sector entities which manage these infrastructures have integrated advanced information and communications technologies into their systems. However, the widespread use and interlinkage of computer and telecommunications throughout these infrastructures has created new

vulnerabilities which, if not addressed, pose significant risks to our national security.

In response to the recommendations included in the PCCIP Report, the Administration in February 1998 created a National Infrastructure Protection Center (NIPC) within the Federal Bureau of Investigation. The NIPC will be composed of the former Computer Investigations and Infrastructure Threat Assessment Center (CITAC), originally funded through the NFIP, and other offices whose responsibilities include operational response to computer intrusion incidents, and indications and warnings for infrastructure and key asset protection. To be successful in performing its mission, the NIPC must rely on the Intelligence Community to provide timely and reliable information regarding possible intrusions, disruptions, and attacks committed by foreign actors on the critical infrastructures.

In its version of the Intelligence Authorization Act for Fiscal Year 1998 the Committee directed the Director of Central Intelligence, the Secretary of Defense, and the Director of the Federal Bureau of Investigation to submit a report articulating a counterintelligence strategy for critical infrastructure protection. The Committee received this report on March 30, 1998. While describing how intelligence agencies have chosen to approach the infrastructure protection issue, this report did not provide a detailed counterintelligence strategy nor did it provide adequate information regarding current or planned counterintelligence activities. With the creation of the NIPC, the Committee believes the Intelligence Community needs a comprehensive strategy to address counterintelligence, threat assessment, indications and warnings, and other intelligence requirements necessary to assist the NIPC in its infrastructure protection mission. Therefore, the Committee directs the Director of Central Intelligence and the Secretary of Defense to perform a joint review to determine the proper role of the Intelligence Community in critical infrastructure protection.

This review should: identify the assets and capabilities of the Intelligence Community which may be of value to the protection of the critical infrastructures; identify which capabilities or technologies useful to intelligence collection or analysis on infrastructure protection are presently lacking within the Intelligence Community, including the capability to provide indications and warnings; provide a counterintelligence strategy designed to protect information regarding vulnerabilities in United States infrastructure; state what, if any, additional collection requirements have been implemented to gain insight into activity against U.S. systems; describe any training programs developed to increase awareness and knowledge of analysts and collectors regarding infrastructure protection concerns; explain how the Intelligence Community will use its expertise and assets to assist the critical infrastructures protection mission of the NIPC and other government entities; and detail how the Intelligence Community will provide timely and actionable intelligence regarding foreign intrusions and attacks to the NIPC and other government entities involved in critical infrastructure protection. This review should also propose how protective techniques and technologies developed or identified by the Intelligence Community may be shared with the private and public sector ac-

tors that manage these infrastructures. The Committee directs that the review of the Intelligence Community's role in infrastructure protection be provided to the Congressional Intelligence Committees not later than March 15, 1999.

Assessment of the Intelligence Community's information infrastructure

In recent years, the Intelligence Community has incorporated advanced computer and telecommunications technologies into its organizations to improve their intelligence collection and analytical capabilities, to increase the productivity of its workforce, and to facilitate communications between different member organizations. As the agencies and offices of the Intelligence Community become more reliant on these technologies, they have become more vulnerable to intrusions, disruptions, and attacks against these systems. The Committee realizes that any breakdown in the information infrastructure of the Intelligence Community will adversely affect its ability to provide timely intelligence to our national security policymakers and military leaders.

To address this potential vulnerability, the Committee directs the Director of Central Intelligence and the Secretary Of Defense to formulate an Intelligence Community information infrastructure security program to ensure the viability and effectiveness of the Intelligence Community's information infrastructure. This program shall develop and implement procedures, practices, policies, and technologies designed to secure and protect the IC's information infrastructure from intrusion, disruptions, and attacks. It should also provide internal controls, audit features, and other necessary elements to address possible insider attacks and other counterintelligence concerns. The Committee directs that the Director of Central Intelligence and the Secretary of Defense forward a report to the Congressional Intelligence Committees not later than March 15, 1999.

The Committee is also concerned that there is no formal, periodic review of the technologies and practices used by the Intelligence Community to provide security and protection for its information infrastructure. Therefore, the Committee directs the Director of Central Intelligence and the Secretary of Defense to perform regular, periodic assessments of the procedures, policies, and technologies implemented by the various intelligence agencies and offices to secure and protect their computer and telecommunications systems. These assessments shall be performed on at least an annual basis. Further, the Committee directs that the Intelligence Community complete an initial series of assessments by the end of fiscal year 1999.

These assessments should include the following: a determination of the adequacy of information infrastructure security procedures and policies; a review of any technologies in use to provide security and/or protect information infrastructure; and the result of aggressive systematic, controlled testing of the Intelligence Community's computer and telecommunications systems for vulnerabilities to intrusion, denial of use, attack, or other disruptive activity. These assessments shall be provided by the Director of Central Intelligence

and the Secretary of Defense to the Congressional Defense Committees not later than March 15, 1999.

DISCLOSURE OF INFORMATION TO CONGRESS

Background and need for legislation

It is not generally known that the "Whistle Blower Protection Act" does not cover employees of the agencies within the Intelligence Community. See 5 U.S.C. §§ 2301 et seq. The "whistle blower" statute also expressly proscribes the disclosure of information that is specifically required by Executive Order to be kept secret in the interest of national defense or the conduct of foreign affairs. Therefore, employees within the Intelligence Community are not protected from adverse personnel action if they choose to disclose such information, irrespective of its classification, to Congress. In fact, an employee who discloses classified information to Congress without prior approval is specifically subject to sanctions which may include reprimand, termination of security clearance, suspension without pay, or removal. See Exec. Order No. 12,958, 60 Fed. Reg. 19825 (1995). Some types of unauthorized disclosures are also subject to criminal sanctions. See 18 U.S.C. §§ 641, 793, 794, 798, 952 (1996); 50 U.S.C. § 783(b) (1996).

In accordance with Executive Order No. 12,958, classified information must remain under the control of the originating agency and may not be disseminated without proper authorization. Consequently, an Executive Branch employee may not disclose classified information to Congress without prior approval. In fact, employees are advised that the agency will provide "access as is necessary for Congress to perform its legislative functions. * * *" "Information Security Oversight Office, General Services Administration, Classified Information Nondislcosure Agreement (SF–312) Briefing Booklet," at 66. In other words, the executive agency will decide what Members of Congress may "need to know" to perform their constitutional oversight functions. The President, in effect, asserts that he has exclusive or plenary authority to oversee the regulation of national security information.

In response to the Administration's position, the Select Committee on Intelligence of the United States Senate reported the Intelligence Authorization Act for Fiscal Year 1998, which included a provision that specifically addressed this issue. See S. 858, 105th Cong., 1st Sess. § 306 (1997). The Senate passed the bill by a vote of ninety-eight to one. Shortly after the Senate vote, the Administration issued a Statement of Administration Policy stating that section 306 was unconstitutional, and that if it remained in the bill in its present form, senior advisers would recommend that the President veto the bill.

Section 306 directed the President to inform all Executive Branch employees that disclosing classified information to an appropriate oversight committee to their Congressional representative is not prohibited by any law, executive order, or regulation or otherwise contrary to public policy, if the employee reasonably believes that the classified information evidences: a violation of any law, rule, or regulation; a false statement to Congress on an issue of material fact; or gross mismanagement, a gross waste of funds, an

abuse of authority, or a substantial and specific danger to public health or safety. This provision was intended to ensure that Congress received information necessary to fulfill its constitutional oversight responsibilities. It was also intended to protect employees from adverse actions based on what was heretofore considered an unauthorized disclosure to Congress.

The Committee intended disclosure to an appropriate oversight committee to mean disclosure to cleared staff or a member of the committee with jurisdiction over the agency involved in the wrongdoing. Members or committee staff who received such information from an employee were to be presumed to have received it in their capacity as members or staff of the appropriate oversight committee. The Committee believed that this presumption was necessary because Members and staff are responsible for ensuring that the information is protected in accordance with committee rules and brought to the attention of the leadership of the committee. The President, by informing Executive Branch employees as directed in section 306, would have authorized disclosure to the appropriate oversight committee or members, thereby recognizing that these committees and members have a "need to know" the information as required by current Executive Branch restrictions on disclosure of classified information.

In conference, members of the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee (SSCI) did not agree to include section 306 as passed by the Senate. The Senate offered to amend section 306, thereby significantly narrowing the scope of the provision to cover only employees of agencies within the Intelligence Community (the Senate-passed version covered all executive employees). The Senate amendment further narrowed the provision by allowing disclosure only to committees with primary jurisdiction over the agencies involved (the original language also allowed disclosure to a Member of Congress who represented the employee).

The Chairman and Ranking Member of the House Committee expressed concern over the possible constitutional implications of such language. They were also mindful of the Administration's veto threat as expressed in the Statement of Administration Policy. The Chairman and vice Chairman of the Senate Select Committee, in deference to their House colleague's concerns, agreed to amend the provision to express a sense of the Congress that Members of Congress have equal standing with officials of the Executive Branch to receive classified information so that Congress may carry out its oversight responsibilities.

The managers' decision not to include section 306 of the Senate bill in the conference report, however, was not intended by either body to be interpreted as agreement with the Administration's position on whether it is constitutional for Congress to legislate on this subject matter. The managers' actions were also not to be interpreted as expressing agreement with the opinion of the Justice Department's Office of Legal Counsel, which explicitly stated that only the President may determine when Executive Branch employees may disclose classified information to Members of Congress. The managers asserted in their Conference Report that members of congressional committees have a need to know information, clas-

sified or otherwise, that directly relates to their responsibility to conduct vigorous and thorough oversight of the activities of the executive departments and agencies within their committees' jurisdiction. Therefore, the President may not assert an unimpeded authority to determine otherwise.

While the managers recognized the Chief Executive's derived constitutional authority to protect sensitive national security information, they did not agree with the Administration that the authority is exclusive. Members of both committees also agreed that whatever the scope of the President's authority, it may not be asserted against Congress to withhold evidence of misconduct or wrongdoing and thereby impede Congress in exercising its constitutional legislative and oversight authority. Therefore, the managers committed to hold hearings on this issue and develop appropriate legislative solutions in the second session of the 105th Congress.

The Senate Select Committee held public hearings on February 4 and 11, 1998 to examine the constitutional implications of legislation such as section 306. The Committee heard from constitutional scholars and legal experts on both sides of the issue. Mr. Randolph D. Moss, Deputy Assistant Attorney General from the Department of Justice Office of Legal Counsel, testified in support of the Administration's position that section 306 and any similar language represents an unconstitutional infringement on the President's authority as Commander in Chief and Chief Executive. Mr. Moss asserted the following:

(A) The President, as Commander in Chief, Chief Executive, and sole organ of the Nation in its external relations has ultimate and unimpeded authority over the collection, retention, and dissemination of intelligence and other national security information.

(B) Any congressional enactment that may be interpreted to divest the President of his ultimate control over national security information is an unconstitutional usurpation of the exclusive authority of the Executive.

(C) The Senate's language vests lower-ranking personnel in the Executive Branch with a "right" to furnish such information to a Member of Congress without prior official authorization from the President or his delegee. Therefore, section 306 and any similar provision is unconstitutional.

The Committee also heard Professor Peter Raven-Hansen, Glen Earl Weston Research Professor of Law from the George Washington University Law School, and Dr. Louis Fisher, Senior Specialist (Separation of Powers) from the Congressional Research Service, testify that the President's authority in this area is not exclusive. Hence, these experts believed that Congress already has authority to regulate the collection, retention, and dissemination of national security information. Professor Raven-Hansen and Dr. Fisher asserted the following:

(A) A claim of exclusive authority must be substantiated by an explicit textual grant of such authority by the Constitution.

(B) There is no express constitutional language regarding the regulation of national security information as it pertains to the President.

(C) The President's authority to regulate national security information is an implied authority flowing from his responsibilities as Commander in Chief and Chief Executive.

(D) As the regulation of national security information is implicit in the command authority of the President, it is equally implicit in the broad array of national security and foreign affairs authorities vested in the Congress by the Constitution. In fact, Congress has legislated extensively over a long period of time to require the President to provide information to Congress.

(E) Congress may legislate in this area because the Executive and Legislative Branches share constitutional authority to regulate national security information.

(F) The Supreme Court has never decided a case that specifically addressed this issue.

(G) The provision is constitutional because it does not prevent the President from accomplishing his constitutionally assigned functions, and because any intrusion upon his authority is justified by an overriding need to promote objectives within the constitutional authority of Congress.

The Committee found the last argument to be persuasive and determined that the Administration's intransigence on this issue compelled the Committee to act.

Following the public hearing on February 11th, the Committee met to mark up a modified version of section 306. One amendment was offered by a member of the Committee and was adopted unanimously. The bill was favorably reported from the Committee on February 23, 1998. The Senate considered the bill (S. 1668) on March 9, 1998 and passed it on a roll call vote of 93 to one. The bill was sent to the House of Representatives and has yet to be considered by that body. Despite assurances by the Chairman and Ranking Member of the Permanent Select Committee on Intelligence of the House of Representatives, the HPSCI has not, as of this printing, held a hearing or met to consider similar legislation. Therefore, in light of the relatively short legislative calendar in this session, the Committee has included this provision in order to give the House of Representatives another opportunity to consider the benefits of this type of legislation.

This bill as passed by the U.S. Senate is contained in title V of this bill and is explained in the section by section analysis.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

TITLE I—INTELLIGENCE ACTIVITIES

Sec. 101. Authorization for appropriations

Section 101 lists departments, agencies, and other elements of the United States Government for whose intelligence and intelligence-related activities the Act authorizes appropriations for fiscal year 1999.

Sec. 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 personnel ceilings for the entities listed in section 101 for fiscal year 1999 are contained in a classified Schedule of Au-

thorizations. The Schedule of Authorizations is incorporated into the Act by this section.

Sec. 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, in fiscal year 1999 to exceed the personnel ceilings applicable to the components of the Intelligence Community under section 102 by an amount not to exceed 2 percent of the total of the ceilings applicable under section 102. The Director may exercise this authority only when necessary to the performance of important intelligence functions or to the maintenance of a stable personnel force, and any exercise of this authority must be reported to the two intelligence committees of the Congress.

Sec. 104. Community management account

Section 104 provides certain details concerning the amount and composition of the Community Management Account (CMA) of the Director of Central Intelligence.

Subsection (a) authorizes appropriations in the amount of $138,623,000 for fiscal year 1999 for the staffing and administration of various components under the CMA. Subsection (a) also authorizes funds identified for the Advanced Research and Development Committee and the Environmental Intelligence and Applications Program to remain available for two years.

Subsection (b) authorizes a total of 283 full-time personnel for elements within the CMA for fiscal year 1999 and provides that such personnel may be permanent employees of the CMA element or detailed from other elements of the United States Government.

Subsection (c) explicitly authorizes the classified portion of the CMA.

Subsection (d) requires that personnel be detailed on a reimbursable basis, with certain exceptions.

Subsection (e) authorizes $27,000,000 of the amount authorized for the CMA under subsection (a) to be made available for the National Drug Intelligence Center (NDIC) in Johnstown, Pennsylvania. Subsection (c) requires the Director of Central Intelligence to transfer the $27,000,000 to the Department of Justice to be used for NDIC activities under authority of the Attorney General, and subject to section 103(d)(1) of the National Security Act. The Committee has also restricted the transfer of the funds authorized in subsection (e) pending the receipt by the congressional intelligence committees of a report mandated in the Intelligence Authorization Act for Fiscal Year 1998.

TILE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Sec. 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of $201,500,000 for fiscal year 1999 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL PROVISIONS

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

Section 301 provides that appropriations authorized by the conference report 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.

Sec. 302. Restriction on conduct of intelligence activities

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

Sec. 303. Extension of application of sanctions laws to intelligence activities

Section 303 extends until January 6, 2000, the authority first granted by section 303 of the Intelligence Authorization Act for Fiscal Year 1996 for the President to delay the imposition of an economic, cultural, diplomatic, or other sanction upon his determination that proceeding with the sanction could compromise an ongoing criminal investigation or an intelligence source or method. This authority was extended until January 6, 1998, by section 304 of the Intelligence Authorization Act for Fiscal Year 1997, and again until January 6, 1999, by section 304 of the Intelligence Authorization Act for Fiscal Year 1998. There is a continuing need for this authority in the event that an automatic or immediate imposition of sanctions would seriously jeopardize a criminal investigation or sources and methods of intelligence collection.

Sec. 304. Extension of authority to engage in commercial activities as security for intelligence collection activities

Section 304 amends section 431(a) of title 10 to extend current Department of Defense authority to engage in commercial activities as security for intelligence collection activities until December 31, 2000.

Sec. 305. Modification of National Security Education Program

Section 305 amends the David C. Boren National Security Education Act of 1991, by adding counter-proliferation studies as an area of primary emphasis in the Act. Section 305 substitutes the Secretary of Energy for the Director of the United States Information Service as a Member of the National Security Education Board, which continues to include the Secretaries of Defense, Education, State, and Commerce, and the Director of Central Intelligence.

Sec. 306. Technical amendments

Section 306 makes technical corrections to section 5(a)(1) and section 6 of the Central Intelligence Agency (CIA) Act of 1949 and section 201(c) of the CIA Retirement Act. The cross-reference in section 5(a)(1) of the CIA Act to subparagraphs (B) and (C) of sec-

tion 102(a)(2) of the National Security Act is no longer current or accurate, and should cite instead to subsections (a)(2) and (a)(3) of section 102. Section 805(a) of the Intelligence Authorization Act for Fiscal Year 1997 (Pub. L. No. 104–293) changed what had been sections 102 (a)(2)(B) and (C) of the National Security Act to sections 102 (a)(2) and (a)(3) of the Act. Similarly, the cross-references in section 5 (a)(1) and section 6 of the CIA Act to "subsection (c)(5) of section 103" and to "section 103 (c)(5) of the National Security Act of 1947 (50 U.S.C. § 403–3 (c)(5));" respectively, are no longer current or accurate. The cross-reference in section 201 (c) of the CIA Retirement Act to that same provision of the National Security Act is also outdated. Section 807 (a)(2) of the Intelligence Authorization Act for Fiscal Year 1997 changed what had been section 103 (c)(5) to section 103 (c)(6) (50 U.S.C. § 403–3 (c)(6)). Section 401 of the present legislation simply updates the cross-references in section 5 (a)(1) and section 6 of the CIA Act and section 201 (c) of the CIA Retirement Act to the pertinent provision of the National Security Act.

TITLE IV—CENTRAL INTELLIGENCE AGENCY

Sec. 401. Extension of separation pay program for voluntary separation of CIA employees

Section 401 amends section 2(f) of the CIA Voluntary Separation Pay Act, Public Law 103–36, 50 U.S.C. § 403–4 note, to extend the Agency's authority to offer separation incentives until September 30, 2001. Without this amendment, the Agency's authority to offer such incentives would expire on September 30, 1999.

The net impact of the six CIA "early out" exercises thus far, along with normal attrition and reduced hiring, has been a significant drop in the Agency's on-duty strength since the separation incentive program began in FY 1993. However, rapid worldwide technological change and increasing concern about such diverse issues as international terrorism, proliferation, drug trafficking, and political instability require the Agency to do more to address the skills mix of the Agency population.

The Agency must continue to reduce or eliminate outdated professions, accelerate the transfer of resources from support to mission-critical work, and hire people with state-of-the-art skills. Voluntary Separation Incentive Pay authority—used for specific, targeted populations—will help the CIA achieve those goals without resorting to involuntary separations in certain occupational categories. The incentive pay would be targeted principally at individuals in outdated occupations and skill categories who would not be separating via regular attrition or switching to another work area after retraining.

Incentive authority through the year 2001 will help enable the Agency to ensure its workforce has the right skills in the right areas at the right time.

Sec. 402. Additional duties for Inspector General of Central Intelligence Agency

Section 402 gives the CIA Office of Inspector General (OIG) responsibility to review and comment in the Inspector General's (IG)

semiannual reports on existing and proposed legislation relating to programs and operations of the Agency. Review and comment by the IG on legislation will complement the IG's responsibility to promote economy and efficiency in Agency programs and operations and will be useful to the DCI and the intelligence committees of Congress as an independent source of analysis.

This function enables the IG to express OIG's views concerning the impact of legislation on the economy and efficiency of Agency activities and the prevention and detection of fraud in such activities. While such a function is implicit in the broad mandate of the Inspector General, the Committee believes that authority for legislative review should be recognized explicitly in the statute.

TITLE V—DISCLOSURE OF CLASSIFIED INFORMATION TO CONGRESS

Sec. 501. Encouragement of disclosure of certain information to Congress

Section 501 is divided into subsections (a) through (d). Subsection (a)(1) directs the President to take appropriate actions to inform the employees of agencies covered in subsection (d) and employees of contractors of such agencies that the disclosure of information described in paragraph (2) to individuals referred to in paragraph (3) is not prohibited by law, executive order, or regulation or otherwise contrary to public policy. In other words, the President is directed to inform "covered employees" that it will not be considered an "unauthorized disclosure" if they provide certain information to Congress, if that information is provided to the appropriate member and the information falls within the specified categories.

Subsection (a)(1) does not, however, define the means by which the President must implement this direction. The Committee refrained from expressly stating the types of actions that the President should take as we have in previous measures. See, e.g., Counterintelligence and Security Enhancements Act of 1994, Pub. L. No. 103–359, title VIII, § 802(a), 108 Stat. 3435 (1994). The Committee has intentionally allowed the President a great deal of latitude to implement this legislation. The Committee does not, however, intend this permissive approach to be interpreted as license ity to promote economy and efficiency in Agency programs and operations and will be useful to the DCI and the intelligence committees of Congress as an independent source of analysis.

This function enables the IG to express OIG's views concerning the impact of legislation on the economy and efficiency of Agency activities and the prevention and detection of fraud in such activities. While such a function is implicit in the broad mandate of the Inspectuch information. This language is consistent with the argument propounded by the Administration in a brief that it filed in the Supreme Court in 1989. See Brief for Appellees, *American Foreign Service Association* v. *Garfinkel,* 488 U.S. 923 (1988) (No. 87–2127). In the *Garfinkel* brief the Department of Justice stated that "the President has uniformly limited access to classified information to persons who have a need to know the particular information, such as a *congressional committee having specific jurisdiction over the subject matter.*" *Id* at 16 (emphasis added).

Paragraph (1)(C) is intended to ensure that members receive information only in their capacity as a member of the committee concerned. The Committee is adamant that any information received by a member of one of the appropriate committees be protected in accordance with that committee's rules for safeguarding classified material and be reported to the committee's leadership. Accordingly, a member is not free to accept covered information as a member of a committee unrestrained by such rules or to withhold knowledge of the information from the committee's leadership. The various national security committees enjoy a long history of trust with the Executive Branch and that record will be continued.

Paragraph (2) defines the type of information that an employee may bring to Congress. It is intended to cover all information in the covered categories, including classified information. Paragraphs (2)(A) and (C) are taken nearly verbatim from the text of the "Whistle Blower Protection Act" and are intended to have the same meaning. See 5 U.S.C. § 2302(b)(8)(A)(i)–(ii) (1994 & Supp. II 1996). The Committee did slightly narrow the language, however, to cover only flagrant abuses of authority. The Committee intended to address only those abuses that are so objectionable as to warrant the attention of Congress.

Paragraph (2)(B) is not found in the "whistle blower" statute and was added to ensure that information pertaining to a false statement to Congress is brought to our attention. In the interest of legislative efficiency, however, the Committee is most concerned with those false statements that pertain to an issue of material fact. The material facts of an issue are those facts that a reasonable person would consider important in reviewing that particular issue. Congress depends on the accuracy of the information provided to it, and when our oversight is based on false information, we must be made aware of it even if the President would prefer to withhold the fact that false information has been provided.

Paragraph (3) refers to the individuals to whom information described in paragraph (2) may be disclosed. Although the Senate Select Committee on Intelligence is composed, inter alia, of members from the Committee on Appropriations, Armed Services, and the Judiciary, we recognize that those committees share jurisdiction with this Committee and each has as its primary responsibilities the oversight of some of the department, agencies or elements of the Federal Government to which such information relates. As noted earlier, the individuals to whom information may be disclosed was narrowed significantly from section 306 of the Intelligence Authorization Act of Fiscal Year 1998 to further ensure the protection of the information.

Paragraph (4) recognizes the inviolability of the rule of secrecy in grand jury proceedings. The Committee does not intend this legislation to circumvent the obligation of secrecy imposed by Rule 6(e) of the Federal Rules of Criminal Procedure and therefore paragraph (1)(A) does not apply to such information. The Committee does not believe, however, that disclosures to Congress fall under the rubric or other statutes that prohibit the disclosure of certain information. The Congress is an entity of the federal government and is capable of protecting such information in the same manner as an executive agency or department. Accordingly, the Committee

does not view a disclosure to Congress as a disclosure outside of the government.

Subsection (b) directs the President to submit a report to Congress on the actions taken under subsection (a). The Committee expects to see a report that describes any procedures established or guidance given to the various agencies, departments, or elements. If the President gives wide discretion to agency heads, the Committee would also like the report to address how each agency or department has implemented this legislation.

Section (c) is intended to protect the integrity of other reporting requirements enacted into relevant law.

Section (d) defines the covered agencies. These are the agencies exempted from the "whistle blower" statute. See 5 U.S.C. § 2302(a)(2)(C)(ii) (1994 & Supp. II 1996).

TITLE VI—FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

Sec. 601. Pen registers and trap and trace devices in foreign intelligence and international terrorism investigations

Section 601 amends the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1802, et seq. (FISA) to authorize pen registers and trap and trace devices in foreign intelligence and international terrorism investigations being conducted by the FBI under guidelines approved by the Attorney General. In particular, it authorizes FISA judges to issue a pen register or a trap and trace order upon a certification that the information sought is relevant to such an ongoing investigation.

The amendment allows the use of pen registers and trap and trace devices in foreign intelligence and international terrorism investigations. Although such devices can be utilized at present, current procedures do not reflect changes in the law since FISA was enacted. Before the use of such device today, the complete FISA predicate for actual interception of the oral or verbal contents on the communication itself must be satisfied. That predicate is designed to satisfy strict constitutional requirements or the conduct of a "search" within the meaning of the Fourth Amendment. However, and subsequent to passage of FISA in 1978, the Supreme Court held in *Smith* v. *Maryland*, 442 U.S. 735 (1979), that accessing numbers dialed to contact another communications facility is not a Fourth Amendment "search". Thus, current procedures impose a standard that is more rigorous than the constitution requires. Section 501 establishes a predicate for the use of pen registers or trap and trace devices that is consistent with that opinion and is analogous to the statutory standard for the use of these devices in criminal investigations. This authority is necessary in order to permit, as is the case in criminal investigations, the use of this very valuable investigative tool at the critical early stages of foreign intelligence and international terrorism investigations.

Unlike the criminal standard, however, this section requires substantially more than mere "relevance" to an ongoing investigation see 18 U.S.C. § 3122(b)(2). In addition to relevancy, the government must also demonstrate that the telephone line involved has been or is about to be used in communication with an international ter-

rorist or a person engaged in clandestine intelligence activities that may involve a violation of law.

Each application must also be approved by the Attorney General or a designated attorney for the Government, with certification by the Federal Bureau of Investigation that the underlying investigation is being conducted under guidelines approved by the Attorney General. It is the committees understanding that the "designated attorney" for the Government will be the Counsel for Intelligence Policy in the Department of Justice. Further delegation of this authority should be done only after the committee is briefed on the compelling need for it.

Applications must be submitted to the Foreign Intelligence Surveillance Court established by FISA; however, the section also allows the designation of Federal magistrates to hear applications for and grant orders approving the installation and use of pen registers or trap and trace devices. This procedure will possibly permit these applications to be heard in a more timely manner and is an appropriate analog to that used in criminal investigations. The committee expects that the exercise of this new authority will be carefully monitored by the Justice Department, and that no magistrates will be designated to hear applications until the committee is briefed on the compelling need to do so, which could be demonstrated, for example, by the number of applications presented to the FISA Court under this new procedure.

Upon request of the applicant, the order authorizing the use of such devices can require that the provider of a wire or electronic communication service, landlord, custodian, or other person not disclose the existence of the investigation or of the pen register until ordered by the Court. The order can also direct hat any records concerning the pen register or trap and trace device held by such persons be maintained under security procedures approved by the Attorney General and the Director of Central Intelligence. These two provisions are identical to existing FISA provisions regarding electronic surveillance and are necessary to protect the FBI's foreign intelligence investigations from disclosure to hostile powers or international terrorist organizations. In addition, the new section includes restrictions or the use of information and the requirement for continuing congressional oversight, similar to provisions in § 106 and 107 of the FISA.

Sec. 602. Access to certain business records for foreign intelligence and international terrorism investigations

Section 602 also amends the Foreign Intelligence Surveillance Act (FISA) by giving the Federal Bureau of Investigation, in conducting foreign intelligence and international terrorism investigations, authority to apply for court orders to obtain records to common carriers, hotels, communications providers, and storage facilities.

Under existing criminal law, grand jury subpoenas may be issued, and the Attorney General has delegated authority to certain Federal agencies in narcotics investigations to issue administrative subpoenas. No analogue to these authorities exists in foreign intelligence and international terrorism investigations. When the FBI seeks common carrier records relating to the clandestine activities

of an agent of a foreign power or an international terrorist, compliance is voluntary, and some entities have chosen not to cooperate.

This new section requires that any or all of the four entities (common carrier, hotel, communications provider, and/or storage facility) comply with a court order based on the certification by the FBI that the records are sought for foreign intelligence purposes, and that there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.

The section also requires that any or all of the four covered entities not disclose the fact that the FBI has sought or obtained the records in question. This is necessary to protect the existence of the investigation from hostile foreign powers or international terrorist groups.

The terms "common carrier," public accommodation facility," "physical storage facility," and "vehicle rental facility" are defined. These are the four entities where the greatest need for compulsory access exists because of their frequent use by subjects of FBI foreign intelligence and international terrorism investigations.

In additional, the section includes provisions for continuing congressional oversight. The committee feels strongly that these provisions are necessary to insure that these new authorities are carefully executed.

COMMITTEE ACTION

On May 7, 1998 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 1999, 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.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXXVI 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 section 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.

○