Calendar No. 528

106TH CONGRESS, *2d Session* | SENATE | REPORT 106–279

AUTHORIZING APPROPRIATIONS FOR FISCAL YEAR 2001 FOR THE INTELLIGENCE ACTIVITIES OF THE UNITED STATES GOVERNMENT AND THE CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM AND FOR OTHER PURPOSES

MAY 4, 2000.—Ordered to be printed

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

REPORT

[To accompany S. 2507]

The Select Committee on Intelligence, having considered the original bill (S. 2507), to authorize appropriations for fiscal year 2001 for intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes, reports favorably thereon and recommends that the bill do pass.

PURPOSE OF THE BILL

This bill will:

(1) Authorize appropriations for fiscal year 2001 for (a) U.S. intelligence activities and programs; (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, 2001, for intelligence activities of the U.S. 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) Prohibit the knowing and willful unauthorized disclosure of classified information to a person not authorized to receive it;

(5) Establish a POW/MIA analytic capability within the Intelligence Community;

79–010 ★ **(Star Print)**

(6) Preclude the application of any U.S. law implementing treaties and other international agreements to otherwise lawful and authorized U.S. Government intelligence activities unless U.S. law expressly states that it will apply to such activities;

(7) Require the Director of Central Intelligence to certify to Congress that each element of the Department of State that handles, retains, or stores material classified at the Sensitive Compartmented Information level is in full compliance with applicable Executive Orders and Director of Central Intelligence Directives;

(8) Permit Executive branch agencies to contribute appropriated funds for fiscal year 2000 to support the Counterdrug Intelligence Executive Secretariat;

(9) Expand the reporting requirements of the CIA Inspector General to include notification concerning certain designated senior officials;

(10) Extend the CIA's Central Services Program and expand the authorities for the Central Services Working Capital Fund;

(11) Permit long-term detailing of CIA employees to the National Reconnaissance Office on a reimbursable basis;

(12) Permit appropriated funds transferred by the CIA to other government agencies for the purpose of the acquisition of land to remain available for a period of three years;

(13) Permit the Director of Central Intelligence to designate categories of employees in addition to those designated in law that would be eligible to receive partial reimbursement for the cost of purchasing professional liability insurance;

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

(15) Support the Intelligence Community's effort to monitor nuclear weapons tests on a worldwide basis by authorizing the Department of Defense to convey nuclear test monitoring equipment to a foreign government through a bilateral agreement which provides the U.S. the right to install, inspect, and maintain such equipment and to have continued access to data collected;

(16) Expand the hiring authority of the Director of Central Intelligence to facilitate the recruitment of eminent experts in science and engineering for research and development projects administered by the National Imagery and Mapping Agency (NIMA), National Security Agency (NSA), National Reconnaissance Office (NRO), and Defense Intelligence Agency (DIA); and

(17) Clarify the standing of United States citizens to challenge the blocking of assets under the Foreign Narcotics Kingpin Designation Act.

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 in-

tent 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 2001 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 monitored compliance with numerous reporting requirements contained in statute. Each report was scrutinized by the Committee and appropriate action was 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's audit staff conducts in-depth audits and reviews of specific programs and activities identified by the Committee as needing thorough and focused scrutiny. The Audit Staff also supports the Committee's continuing oversight of a number of administrative and operational issues. During the last year the Committee's Audit Staff reviewed the National Imagery and Mapping Agency (NIMA) and a covert action program; completed portions of the Committee staff's review of counterintelligence at the Department of Energy's National Laboratories and the mishandling of classified information by former Director of Central Intelligence John Deutch; and monitored the products and activities of the Community's statutory and adminis-

trative Inspectors General. These kinds of inquiries frequently lead to Committee action with respect to the authorities, applicable laws, and budget of the activity or program concerned.

COMMITTEE RECOMMENDATIONS

The 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 over, and priorities for, intelligence programs and activities public to the greatest extent possible consistent with the nation's security. The Committee, therefore, has included in this report information that is unclassified.

TECHNICAL ADVISORY GROUP (TAG)

In 1997, the Committee established a Technical Advisory Group (TAG) to inform and advise Members of the threats and opportunities presented by the extraordinary technological advances of recent years. The TAG members have extensive expertise in computer hardware, software, telecommunications, aviation, satellites, imagery, physics, chemical engineering, and other technical fields, as well as, in many cases, extensive Intelligence Community experience. They are drawn from both government and industry, and volunteer their time and effort to help the Committee understand how the Intelligence Community is being affected by, and can take advantage of, current and developing technologies.

The Committee wishes to thank the TAG members for the many hours they devoted to examining Intelligence Community capabilities. The Committee will continue to study the findings of this distinguished group, to draw upon their world-class expertise, and to work with the Director of Central Intelligence to implement the Committee's recommendations that are based in whole or in part on the findings of the TAG.

Signals Intelligence

In 1997, at the Committee's behest, the TAG undertook a study of the National Security Agency (NSA). The NSA has responsibility for collecting signals intelligence (SIGINT) from electronic signals worldwide, and therefore requires an in-depth understanding of the global telecommunications revolution to complete its mission. The TAG extensively reviewed current and planned operations as well as research and development programs at the NSA. Their findings and recommendations regarding the NSA's ability to address a changing technological environment have been incorporated into prior and current Committee initiatives.

This year, the Committee asked the TAG to update its SIGINT review in light of reforms both proposed and underway at the NSA. The Committee has again utilized the TAG's analysis and recommendations for guidance in drafting the Intelligence Authorization Act for Fiscal Year 2001.

Human Intelligence

In 1998, the Committee asked the TAG to review the status of the Intelligence Community's human intelligence (HUMINT) capabilities. The TAG concluded that human intelligence collection will play an increasingly important role in defending U.S. national security interests and recommended that the Intelligence Community develop a comprehensive plan that recognizes the rapidly changing and technically sophisticated world that now confronts the HUMINT collector.

This year, the Committee also asked the TAG to assess the progress that the Intelligence Community has made in undertaking the substantial changes to HUMINT recommended in 1998. The results of this review have been incorporated, where applicable, within this year's authorization.

MASINT and IMINT Intelligence

In 1999, the TAG reviewed the Intelligence Community's capabilities to collect measurement and signature intelligence (MASINT) and imagery intelligence (IMINT). The Committee referred often to the TAG's review of MASINT and IMINT as it drafted the Intelligence Authorization Act for Fiscal Year 2000. Some of the TAG's conclusions have influenced provisions within this year's bill as well.

COMMITTEE PRIORITY ISSUES

Rebuilding the National Security Agency

The Committee is increasingly troubled by the National Security Agency's (NSA) growing inability to meet technological challenges and to provide America's leaders with vital signals intelligence (SIGINT). Successful execution of the NSA's mission is essential to protecting U.S. national security. The Committee is committed to providing the resources and support necessary to restore and improve the NSA's capabilities.

Collecting and deciphering the communications of America's adversaries has been instrumental in protecting our national security during the last half of the 20th Century. SIGINT has played a decisive role in every military confrontation in which the United States has been involved, from World War II through the Kosovo conflict. SIGINT also has consistently provided our nation's policy makers with additional knowledge and understanding of international developments and threats to the nation's security. This essential intelligence information has enlightened our foreign policy, thwarted terrorist attacks, disrupted narcotics trafficking, and averted unnecessary military conflict. American presidents and senior policy makers rely upon this vital source of information to make critical decisions on behalf of the national interest.

As the central repository of the government's SIGINT expertise, the NSA is a critical national asset. The NSA historically has led the way in development and use of cutting edge technology that has kept the United States a step ahead of those whose interests are hostile to our own. Unfortunately, in recent years, the Administration has failed to invest in the infrastructure and organizational

changes required to keep pace with revolutionary developments in the global telecommunications system.

As detailed above, in 1998, and again this year, the TAG reviewed the NSA's operations. The TAG's conclusions are disturbing. While the current information revolution presents both opportunities for and threats to its mission, the NSA's ability to adapt to this changing environment is in serious doubt. The TAG's two reports identified serious deficiencies resulting from the sustained budget decline of the past decade. As resources have been reduced, the NSA systematically has sacrificed infrastructure modernization in order to meet day-to-day intelligence requirements. Consequently, the organization begins the 21st Century lacking the technological infrastructure and human resources needed even to maintain the status quo, much less meet emerging challenges.

This year's TAG review, however, sounded a note of optimism, noting that the NSA Director in November 1999 initiated an aggressive and ambitious modernization effort. In November 1999, the Director began a series of changes designed to transform the NSA and sustain it as a national asset. Spurred by the NSA computer outage in January 2000, this transformation includes sweeping organizational and business strategies that promise to transform the way the NSA conducts its missions. The Committee is encouraged by these actions, and expects that the Director of Central Intelligence and the Secretary of Defense will support the Director of the NSA in making the difficult decisions necessary for the NSA to restore its predominance. To return the NSA to organizational and technological excellence, NSA managers, as well as Intelligence Community leaders and the Congressional oversight committees, must be prepared to accept a level of risk as some resources are shifted from short-term collection to long-term infrastructure modernization. Failure to do so will irreversibly undermine the NSA and its ability to perform in a transformed global information technology arena.

To address these problems, the TAG recommended new business practices coupled with additional resources to finance this recovery. Inadequate National Foreign Intelligence Program (NFIP) spending leaves little flexibility to meet the increasingly complex intelligence challenges faced by the NSA, but the crisis demands immediate attention and warrants shifting resources in order to stave off a steady and inevitable degradation of the NSA's unique and invaluable capabilities. The budget recommendations in the classified annex accompanying this bill constitute a down payment on this requirement.

The Committee supports the NSA Director's transformation objectives, and recommends investments in areas that are consistent with his plan. The Committee is particularly encouraged by the willingness of the Director to reach beyond his current workforce to hire industry professionals. The Director has hired a Chief Financial Manager from industry, an essential prerequisite if the NSA is to develop a comprehensive business plan for this effort. As the Director moves forward on his plan to reshape the Agency, the Committee will look for specific goals to support establishment of business-based objectives.

Despite the need for additional resources, the Committee does not believe that money alone will solve the NSA's problems. Organizational change also is essential. The Director of the NSA has authority over approximately thirty percent of the total SIGINT budget within the NFIP. Other agencies and organizations within the NFIP and the Department of Defense expend funds for cryptologic activities outside the authorities of the Director of the NSA. If the Director of the NSA is to have functional responsibility for rebuilding the nation's cryptologic program, the Director must have greater authority in the planning, programming, budgeting, and execution of the entire SIGINT budget. To build a comprehensive, efficient U.S. Cryptologic System, the NSA Director must have the requisite authorities to manage his program. The Committee will work with the Director to improve his ability to provide centralized direction across the SIGINT infrastructure as he implements his modernization strategy.

Rebuilding the NSA is the Committee's top priority. Failure to do so risks our nation's security. The Committee, therefore, will take whatever steps are necessary to ensure America's continuing superiority in the signals intelligence field.

Tasking, Processing, Exploitation, and Dissemination Funding Shortfall

The Committee has long been concerned that intelligence collection continues to outstrip analysis, and is troubled that funding for the latter remains woefully inadequate. This funding shortfall challenges the Intelligence Community's ability to manage the tasking, processing, exploitation, and dissemination (TPED) of intelligence collected by satellites, airplanes, unmanned aerial vehicles, and other platforms and sensors. The issue of TPED is at the heart of how the Intelligence Community collects raw intelligence data, and then in a timely manner, turns it into a product that is understandable and usable to a wide variety of consumers, from the President of the United States to the military commander in the field.

In June 1999, the National Imagery and Mapping Agency (NIMA) issued a congressionally-mandated report describing the challenges and projected shortfalls in the areas of TPED of intelligence to be collected by the Future Imagery Architecture (FIA) satellite program and other intelligence collection systems. The funding shortfall figures in the NIMA report were updated in the summer of 1999.

The NIMA report addressed only Phase I of three phases identified by the Intelligence Community's TPED assessment process. The three phases of TPED modernization are defined and staged in the following manner:

• *Phase One—Infrastructure Foundation:* covering fiscal years 2001–2005, this portion of the TPED modernization plan will (a) provide full support to the Enhanced Imagery System (EIS); (b) provide a foundation for the FIA; (c) provide infrastructure "hooks" for commercial imagery; and (d) provide a minimal level of modernization supporting airborne systems.

• *Phase Two—Imagery and Geospatial Information Transition:* covering fiscal years 2002–2007, this portion of the TPED mod-

ernization plan will (a) provide full support for the FIA; (b) provide full support for commercial imagery; (c) provide intermediate modernization supporting airborne systems; (d) expand the ability to handle motion imagery; and (e) provide infrastructure "hooks" for TPED modernization supporting all intelligence collection ("multi-INT"), including signals intelligence, human intelligence, and measurement and signature intelligence.

• *Phase Three—Common Operational Picture:* covering fiscal years 2004–2009, this portion of the TPED modernization plan will (a) provide full support for multi-INT TPED; (b) provide support of all sensor platforms; (c) integrate moving target indicator (MTI) data; and (d) provide full support for airborne systems.

The updated NIMA modernization plan for Phase One contains 26 recommendations for TPED modernization with associated cost estimates to implement each. The multi-billion dollar modernization plan sets forth an overall cost ranging from implementing only the Imagery and Geospatial Community's highest priority TPED improvements to full funding of all 26 recommendations over the next five years.

Complete Phase Two and Phase Three cost estimates have not yet been developed and are expected to be formulated in the context of the fiscal year 2002 and fiscal year 2004 budget cycles, respectively. Preliminary indications are that each phase will carry a significant price tag over and above the funding range currently estimated for Phase One.

The funding contained in the proposed fiscal year 2001 budget for Phase One TPED modernization is about 10% of the total funding amount pledged by the Administration for the effort over the next five years. A proportionate, one-fifth, installment of the total amount pledged would have required a funding commitment in fiscal year 2001 nearly double the amount actually proposed.

The inadequacy of the fiscal year 2001 TPED funding request is more stark when compared to the needs set forth in the NIMA's updated TPED modernization plan. The fiscal year 2001 request for NIMA TPED is significantly below what is required in the upcoming year to support only the top priorities in the modernization plan. This shortfall balloons when compared to the funds needed to proceed with all the recommended fiscal year 2001 TPED improvements. When expressed in percentage form, the proposed funding in fiscal year 2001 for NIMA TPED is 25% of what is required for the top priorities alone, and 15% of what is required for the full complement of modernization projects.

The recently completed Defense Science Board Task Force report on NIMA also found the TPED modernization funding plan to be insufficient and recommended an investment of $3 billion over the next five years in order for the U.S. to maintain information superiority in the future.

The Committee concludes that Phase One of the TPED modernization plan is woefully underfunded in the proposed fiscal year 2001 budget and over the Future Years Defense Plan (FYDP), i.e., fiscal years 2001–2005. The Committee is troubled by the Administration's unwillingness to recognize the significant disparity between its proposed funding plan and the TPED modernization funding plan, which is based on a rigorous technical evaluation

that has yet to be challenged as being either flawed or inflated. The proposed funding for the TPED modernization effort to date has come from anticipated savings from lower than expected inflation over the next five years and not from other programs within the Intelligence Community and defense budgets, thus avoiding the tough programmatic trade-offs and choices required to fully fund needed modernization.

The Committee is concerned that the dramatic underfunding of Phase One TPED modernization in fiscal year 2001 is setting up a budgetary crunch wherein a disproportionate amount of funds will be required in subsequent years of the FYDP. Assuming the budgetary top line for national security is not increased over this period of time to cover the emerging TPED modernization bill, these out-year balloon payments will create a Hobson's choice for the Intelligence Community: either make abrupt and deep cuts in other needed programs or curtail the TPED modernization program to an extent that raises serious doubt as to why tens of billions of dollars are being spent on intelligence collection platforms when the customers of the intelligence will not be able to use much of the raw data that is collected. The Committee cannot and will not accept either alternative.

When the yet unknown costs for the Phase Two TPED modernization effort covering fiscal years 2002–2007 and the Phase Three TPED modernization effort covering fiscal years 2004–2009 are added to the equation, this chasm widens as does the challenge to find the needed funding to bridge it.

Therefore, the Committee recommends a number of funding changes within the NIMA budget, both in the National Foreign Intelligence Program and the Joint Military Intelligence Program, to bolster Phase One TPED modernization efforts in fiscal year 2001. These funding changes are described in the classified annex to this Report.

MISHANDLING OF CLASSIFIED INFORMATION BY FORMER DCI DEUTCH

The Committee was deeply concerned to learn of serious breaches of security by former Director of Central Intelligence (DCI) John M. Deutch. As the DCI, Mr. Deutch was entrusted with protecting our nation's most sensitive secrets pursuant to the National Security Act of 1947, which charges the DCI to protect the sources and methods by which the Intelligence Community conducts its mission. It is this Committee's view, based upon the Committee's inquiry to date, that Mr. Deutch failed in this responsibility. Mr. Deutch, whose conduct should have served as the highest example, instead displayed a shocking and reckless disregard for the most basic security practices required of thousands of government employees throughout the CIA and other agencies of the Intelligence Community. In open testimony before the Committee, current DCI George Tenet stated, "there was enormously sensitive material on [Mr. Deutch's] computer, at the highest levels of classification."

The Committee believes further, based upon the Committee's inquiry to date, that, in their response to Mr. Deutch's actions, Director Tenet, Executive Director Nora Slatkin, General Counsel Michael O'Neil, and other senior CIA officials failed to notify the

Committee in a timely manner regarding the Deutch matter, as they are required by law to do.

The Committee has determined that there are several gaps, or potential gaps, in existing law that require legislative action. The Committee has decided to proceed with one statutory change at this time (Section 401, described below), despite the fact that the Committee has not completed its inquiry, because there is broad agreement on the nature of, and the solution to, this particular problem. The Committee also wishes to ensure that this amendment can be enacted into law expeditiously as part of the Intelligence Authorization Act for Fiscal Year 2001. The Committee is reviewing additional proposals for statutory changes, and may make recommendations when the Committee completes an unclassified report setting forth the Committee's findings and conclusions.

Inspector General reporting requirements relating to senior CIA officials

Section 401 of the Intelligence Authorization Act for Fiscal Year 2001 closes gaps in the Congressional reporting requirements to the intelligence committees revealed by the Deutch matter. Current law requires the Inspector General to notify the committees "immediately" if the Director or Acting Director, but not the *former* Director, is the subject of an Inspector General inquiry. The committees were not notified of the security breach by Mr. Deutch until more than 18 months after it was discovered, and even then the full scope of the problem was not adequately disclosed. This amendment broadens the notification requirement to include former DCIs, all Senate confirmed officials (Deputy Director of Central Intelligence, Deputy Director of Central Intelligence for Community Management, Assistant Directors for Central Intelligence, and General Counsel), the Executive Director and the Deputy Directors for Operations, Intelligence, Administration, and Science and Technology. In addition to expanding the number of senior officials covered by the notification requirement, the amendment also requires the IG to notify the intelligence oversight committees whenever one of the designated officials is the subject of a criminal referral to the Department of Justice.

STATE DEPARTMENT SECURITY AND COUNTERINTELLIGENCE

Limitation on Retention or Storage of Certain Classified Materials by the Department of State

In the last two years, the Committee has taken a series of steps designed to identify, and require the State Department to address, serious deficiencies in policies, procedures, and attitudes relating to the protection of classified information. Despite these efforts, and a nascent, if belated, recognition by the State Department of the magnitude and severity of the problem, serious breakdowns in security and counterintelligence practices continue to occur.

Most recently, on April 17, 2000, *The Washington Post* published an article entitled "State Dept. Computer with Secrets Vanishes." According to this article and subsequent press reporting, a laptop computer containing highly sensitive classified intelligence materials, including Sensitive Compartmented Information (SCI) relat-

ing to weapons proliferation, has disappeared from the State Department Bureau of Intelligence and Research (INR), and is presumed stolen. The FBI is investigating the matter. The Committee has been briefed by the Department of State, the CIA and the FBI.

The loss of this information, which endangers intelligence sources and methods directed at one of our most critical intelligence targets, is a matter of urgent concern. The Committee expects that the FBI will thoroughly pursue all aspects of this loss, including a full counterintelligence investigation.

In addition to security and counterintelligence issues with regard to the loss of the classified laptop, the Committee also was distressed at the failure of the State Department, and the CIA, to notify the Congressional intelligence committees about this incident—even after the story appeared in the press. The State Department had known of the loss for almost three months. The CIA became aware of the loss of the computer in mid-February.

Section 502 of the National Security Act [50 U.S.C. 413a] requires that the heads of all departments of the United States Government involved in intelligence activities keep the intelligence committees "fully and currently informed of all intelligence activities," including "significant intelligence failures." Clearly, the loss and possible compromise of highly sensitive compartmented intelligence information should be considered a significant intelligence failure and should have been reported in a timely manner to this Committee and the House Permanent Select Committee on Intelligence.

Beyond the clear legal requirement for notification, we note that the State Department is well aware of this Committee's sustained interest in security and counterintelligence problems at INR and the Department at large, and therefore should have informed us of this event even in the absence of a statutory requirement.

The January 2000 laptop incident follows the discovery of a Russian listening device in a seventh floor State Department conference room. On December 8, 1999, the FBI detained a Russian intelligence officer, Stanislav Gusev, as he was recording transmissions from a bug implanted in a piece of chair rail, in a conference room within the Department of State headquarters building. Gusev was declared *persona non grata* and required to leave the United States.

Gusev's expulsion capped a six-month investigation that began when the FBI spotted the Russian intelligence officer loitering near the State Department. Following surveillance and observation of Gusev, technical countermeasures discovered the remotely-activated device in the conference room.

The FBI and State Department continue to investigate who was responsible for planting the bug, and what sensitive materials discussed in the conference room may have been compromised. Recreating the extent to which Russian intelligence or other personnel may have had access to the room in question has been complicated by the fact that from 1992 until August 1999, there were no escort requirements for Russian (or other foreign) visitors to the State Department.

The Gusev incident followed a February 1998 incident, in which an unidentified man wearing a tweed jacket entered the Secretary

of State's seventh floor office suite and removed classified documents, including SCI documents. He has never been identified, the documents have never been recovered, and poor procedures for handling classified information resulted in the Department's inability to reconstruct which documents were taken.

Following the "tweed jacket" affair, the SSCI, in the Annex to the Intelligence Authorization Act for Fiscal Year 1999, directed the State Department Inspector General (IG) to review and report on State Department policy and procedures for handling classified information within the State Department Headquarters facility.

The resulting IG report, entitled *Protecting Classified Documents at State Department Headquarters,* found that "[t]he Department [of State] is substantially *not* in compliance with the DCIDs [Director of Central Intelligence Directives] that govern the handling of SCI." *(emphasis in original)* According to the Report:

- "Very highly classified documents relating to intelligence reporting are not safeguarded in accordance with government regulations. Most offices have never been inspected and accredited for handling such documents.
- A significant number of foreign nationals are permitted unescorted access to the Department. Uncleared maintenance, repair, and char force personnel are not always escorted in areas where classified information is handled, processed, stored, and discussed.
- Administrative actions taken to discipline employees are ineffective to ensure that poor security practices are corrected.
- Unit security officers are not well informed about security requirements and do not have the authority to enforce security requirements."

In response to the IG Report, in the Annex to the Intelligence Authorization Act for Fiscal Year 2000, the Congressional intelligence committees fenced funds for the State Department Bureau of Intelligence and Research pending receipt of (1) a State Department report on specific plans for enhancing the security of classified information within the State Department and fully implementing, as appropriate, the recommendations found within the Inspector General's report, and (2) a report from the Director of Central Intelligence (DCI) evaluating the State Department's compliance with all DCIDs related to the protection of Sensitive Compartmented Information. These reports were provided to the Congressional committees in February of this year. The State Department, in its response, identified a number of actions or proposed actions it intended to take in response to the IG Report.

The DCI report noted that an independent review by the CIA and the Community Management Staff confirmed that the State Department was not in compliance with applicable DCID requirements, and concluded that certain additional steps were required to "improve security practices in Department offices where SCI is handled and discussed as well as to strengthen SCI document control and accountability." The Department agreed with the findings of the DCI report as to the steps required to address these deficiencies.

In addition, in the wake of the Gusev incident, Secretary Albright ordered a "top-to-bottom" review of the Department's secu-

rity practices and procedures led by Assistant Secretary for Diplomatic Security David Carpenter. The review is expected to be completed in the near future. The Committee looks forward to receiving the presentation of a comprehensive plan that will ensure that security and counterintelligence receive adequate resources and consistent senior management attention.

Despite the February 2000 report confirming that the State Department failed to comply with applicable DCID requirements, the DCI decided to permit the CIA and other Intelligence Community components to continue to provide SCI materials to INR and other authorized recipients at the Department of State. The Committee believes, however, that the time has come for the State Department to be held accountable for its failure to comply with directives governing the protection of SCI information.

The Committee therefore has adopted a provision, Section 306 of the Intelligence Authorization Act for Fiscal Year 2001, that would require the DCI to certify to the Congressional intelligence and foreign affairs committees whether each element of the State Department that handles, retains or stores classified information that is classified as SCI complies with all applicable DCI directives (DCIDs) and all applicable Executive Orders relating to the handling, retention, or storage of such classified information. Moreover, the DCI may not certify, as in compliance, any element that is operating under a DCI waiver of compliance with respect to any such directive or Executive Order. The DCI must promptly notify the Congressional intelligence and foreign affairs committees if the DCI determines that any element is not in full compliance.

Unless the DCI has certified each covered element of the Department of State to be in full compliance, the following restrictions take effect as of January 1, 2001: (1) no funds authorized to be appropriated under the Intelligence Authorization Act for Fiscal Year 2001 may be obligated or expended by the Bureau of Intelligence and Research of the Department of State, until each covered element has been determined to be in full compliance, and (2) no covered element that has not been certified to be in full compliance may retain or store SCI material, until the DCI has certified that it is in full compliance.

The provision further stipulates that the President may waive the application of the restriction on the retention or storage of classified information if the President determines that such a waiver is in the national security interests of the United States. The President must provide to the Congressional intelligence and foreign affairs committees a report with respect to any such waiver, describing the element affected, the reasons for the waiver, and the actions taken by the President to protect covered classified material to be handled, retained, or stored by the element in question.

Department of State Inspector General Review

The Committee anticipates that the Department will come into compliance with applicable DCIDs in the near future. There will be a need for continued monitoring and oversight to ensure ongoing compliance, however. Therefore, the Committee directs the Department of State Office of Inspector General to conduct reviews of State Department policies and procedures for protecting classified

information at Main State Headquarters annually for the next five years, beginning with a report to be submitted by December 31, 2001. As in the September 1999 report, the Committee expects the State IG to determine, among other matters, compliance with Director of Central Intelligence Directives (DCIDs) regarding the storage and handling of Sensitive Compartmented Information (SCI) material.

Transfer of SCI Authority at the Department of State

In 1998, the Committee directed a State Department Office of Inspector General review of the protection of classified information at the Department of State, and last year the Committee directed a review by the Director of Central Intelligence Department compliance with directives regarding protection of classified material. Among the State IG recommendations included in its review was the transfer of responsibility for protection of Sensitive Compartmented Information (SCI) from the Bureau of Intelligence and Research (INR) to the Bureau of Diplomatic Security (DS). The DCI review did not address this recommendation. The Committee believes such a transfer unnecessarily complicates efforts to address this issue, and may hinder the possibility for success in this vitally important task.

The transfer of responsibility for protection of SCI material from INR to DS improperly transfers authority from an Intelligence Community element to a bureau over which the Director of Central Intelligence has no oversight authority. Despite INR's record, it is a member of the Intelligence Community, and the DCI has statutory authority to approve its budget. This oversight and budgetary authority will be critical to ensure effective implementation of measures to protect intelligence information. The DCI does not approve the budget request for DS, has no influence over DS personnel, and will not have the organizational authority to review directly DS compliance with directives concerning the handling of classified information. This will severely limit the ability of the DCI to carry out his responsibility under the National Security Act of 1947 to ensure the protection of intelligence sources and methods.

Further, the proposed transfer will complicate and hinder oversight of protection of SCI material at the State Department by the Legislative branch. This Committee and the House Permanent Select Committee on Intelligence (HPSCI) are the congressional bodies with the legal responsibility, institutional knowledge, and expertise necessary to exert legislative oversight over the protection of SCI material. The SSCI and HPSCI are charged with overseeing the Intelligence Community, which produces the SCI material that requires stringent controls and accounting. Neither the SSCI nor the HPSCI currently have direct jurisdiction or oversight over the Bureau of Diplomatic Security.

For the reasons stated above, the Committee believes the proposed transfer of the responsibility for protection of SCI material from INR to DS imprudently takes this function away from those with the authority to ensure successful implementation. Therefore, the Committee will closely review any Department of State plan to transfer the responsibility for protecting Sensitive Compartmented

Information from the Bureau of Intelligence and Research to the Bureau of Diplomatic Security. The Committee supports the efforts by the Secretary of State to improve the security procedures and practices throughout the State Department. However, the Committee believes the responsibility for protecting SCI material within the Intelligence Community elements that use and produce such information must continue to reside with those elements themselves.

COUNTERINTELLIGENCE—CI 21

The Committee has become increasingly concerned about the ability of existing U.S. counterintelligence structures, programs, and policies to address both emerging threats and traditional adversaries using cutting edge technologies and tradecraft in the 21st Century. The Committee has made its views known to the nation's senior intelligence and counterintelligence officials, and found many of them share these concerns.

On March 8, 2000, the Director of Central Intelligence, the Director of the FBI, and the Deputy Secretary of Defense unveiled a proposal entitled "Counterintelligence for the 21st Century" during a closed hearing before the SSCI. The plan, generally referred to as "CI 21," resulted from a review launched in June 1999 to assess existing counterintelligence structures and capabilities to address emerging as well as traditional counterintelligence threats.

CI 21 restates and expands upon other recent assessments of the emerging counterintelligence environment. The report notes that the threat has expanded beyond the traditional paradigm of "adversary states stealing classified data"—which includes traditional espionage by Russia, the PRC, North Korea, Cuba, Iran, and Iraq—to include new efforts by these traditional adversaries, as well as threats from certain allies and friendly states, to collect economic information and critical but unclassified technologies.

Terrorist groups, organized crime, and drug cartels are additional, non-state actors that pose an increasing counterintelligence threat. New roles and missions for U.S. military forces, such as peacekeeping and new kinds of coalition operations, create new force protection and counterintelligence challenges. Academic exchanges and joint ventures also are venues for the loss—witting or unwitting—of sensitive or even classified information.

Both traditional and non-traditional threats are exploiting modern technology, particularly modern computer technology and the Internet, to develop information warfare (IW) and intelligence collection capabilities and tradecraft that alter traditional notions of time, distance and access.

Complicating the task of U.S. counterintelligence agencies is the sheer volume of classified and sensitive information that requires protection, and the resulting need for top level policy guidance and prioritization in determining which information and technologies must be protected.

CI 21 found current U.S. counterintelligence capabilities intended to confront this expanding and changing threat to be "piecemeal and parochial." Key problems include:

- inadequate coordination between policy and counterintelligence, including failure to identify "must protect" information;
- inadequate coordination, cooperation, and information-sharing between counterintelligence agencies;
- lack of strategic counterintelligence threat analysis;
- lack of agility, and a focus that is reactive instead of proactive—at both the national and operational levels;
- failure to adequately exploit new technologies;
- lack of a national counterintelligence plan to integrate information, analysis, and a new proactive focus;
- an inadequately prepared workforce and insufficient, diffused resources;
- a lack of a national advocate for resources, policies, and proactive initiatives; and
- inadquate coordination with the private sector.

To address these shortfalls, the CI 21 report recommends adoption of a new counterintelligence philosophy—described as more policy-driven, prioritized, and flexible, with a strategic, national-level focus—and a restructured national counterintelligence system. The proposed new national counterintelligence system would include:

- A National Counterintelligence Executive;
- A National Counterintelligence Board of Directors; and
- A National Counterintelligence Steering Committee.

The Committee commends both the senior leadership and the senior counterintelligence officials of the CIA, FBI, and the Defense Department for their work in developing the CI 21 proposal. This ambitious plan proposes significant changes in the way the United States Government approaches, and organizes itself to meet, the threat of foreign espionage and intelligence gathering. Implementation would require additional resources, as well as changes to existing Presidential directives and statutory authorities. Perhaps most difficult, it would challenge traditional ways of doing business.

The Committee notes that the CI 21 plan has not yet received final interagency approval. Given the seriousness and evolving nature of the threat, and the demonstrated shortcomings of current counterintelligence structures, the Committee strongly urges the agencies involved to reach agreement on this matter.

COUNTERINTELLIGENCE—DEPARTMENT OF ENERGY

Following its extensive 1999 review of Department of Energy (DOE) security and counterintelligence problems, the Committee continues its oversight over the Department's Counterintelligence and Intelligence programs. The Committee is monitoring closely the Department's implementation of Presidential Decision Directive-61 (PDD), the DOE Counterintelligence Implementation Plan and the National Defense Authorization Act of Fiscal Year 2000 to ensure that the Department follows through on these and other long-overdue reforms. Although the Committee understands that the Department's problems are deeply-rooted and will not be solved overnight, the Committee is disappointed that in the Department's initial counterintelligence inspections of the major weapons laboratories, only one lab—Lawrence Livermore National Laboratory—re-

ceived a "Satisfactory" rating. Sandia National Laboratories received an "Unsatisfactory" grade, while Los Alamos National Laboratory was judged "Marginal."

The Committee is also concerned that, to date, neither the DOE Director of Counterintelligence, the DCI, nor the FBI Director has been able to certify to the Congress, pursuant to Section 3146(b) of the National Defense Authorization Act for Fiscal Year 2000, that the foreign visitors program at any one of the national laboratories: complies with applicable DOE orders, regulations, and policies, and PDD and similar requirements, relating to the safeguarding and security of sensitive information; fulfills counterintelligence responsibilities arising under such requirements or Directives; has adequate protections against the inadvertent release of Restricted Data or other sensitive information; and does not pose an undue risk to the national security of the United States.

The results of the DOE counterintelligence inspections, which will make it difficult indeed to make the certifications set forth under Section 3146, underline the extent and resilience of the problems identified at the Department of Energy. They also reinforce the need for continued vigorous executive leadership at the Department, together with aggressive Congressional oversight, to ensure that the current momentum for reform is maintained.

MANAGEMENT OF MASINT

The Committee has repeatedly noted the significant contribution that measurement and signature intelligence (MASINT) can make in accomplishing critical missions within the Intelligence Community, particularly in countering proliferation of weapons of mass destruction. As a result, the Congress has specifically designated a significant amount of additional funds provided over the last three years to bolster MASINT capability. At the same time, the Congress and various independent entities, including the Department of Defense (DOD) Inspector General, have criticized the Intelligence Community for failing to come to grips with resources, management, and organizational MASINT deficiencies. Therefore, the Committee was not surprised to learn that during its first real combat test in Kosovo, MASINT performed poorly. The January 31, 2000, Kosovo/Operation Allied Force After-action Report stated that MASINT's "flaws in supporting tasking, processing, exploitation, and dissemination limited their overall utility and needed to be corrected to make these capabilities an integral part of intelligence support to operations."

The Committee believes that the continued lack of adequate management within the Intelligence Community for the MASINT program has been demonstrated by the failure to sustain Congressional priorities, especially in the General Defense Intelligence Program (GDIP). The Committee is concerned with the funding shortfalls in individual programs that have not been addressed as part of a comprehensive plan.

At the same time, the Committee also recognizes that the capitalization of these sensors appears to be beyond the capability of the GDIP as it is currently constituted and resourced by the Administration. The Committee also questions whether the Cold War orientation of many of these sensors, and level of funding required

to maintain them, is reflective of the current realities regarding transfer and proliferation. Rather than a piecemeal approach to recapitalization, it seems prudent to the Committee to direct a review of the technical collection "system of systems," with particular emphasis on articulating the requirements base, programmatic status, operations and maintenance costs, and the Administration's approach to recapitalizing or reconfiguring the current systems. The review should be conducted by the DCI, in conjunction with the GDIP Program Manager and the Director of the Central MASINT Organization, and result in a report to be delivered to the Committee no later than October 1, 2000. As far back as 1993, this Committee has expressed its displeasure with the management of MASINT. The Intelligence Authorization Act for Fiscal Year 1994, noted that "[t]he Senate has been critical of the performance of the Central MASINT Office (CMO) to date and concerned that the Director, DIA, did not have the interest or authority to manage a major but uncoordinated and underdeveloped discipline." Little, other than the organization's name, has changed and intelligence support to our operational forces is now suffering.

Last year, the Committee concurred with the findings and recommendations of its Technical Advisory Group (TAG). In their report, the TAG recommended the creation of a new high-level organization, led by a world-class expert and staff detailed from operational elements to facilitate deployment of technologies on an urgent basis. The Senate and House Conferees noted the importance and potential offered by MASINT technologies—if they are rigorously developed and rapidly deployed. The Conferees specifically noted that, (1) successful exploitation of MASINT technologies could significantly enhance U.S. national security; (2) MASINT technologies could potentially eclipse in value the more traditional intelligence disciplines; (3) MASINT technologies offer potential solutions to denial and deception capabilities and other countermeasures; and (4) the IC currently lacks a sufficiently robust MASINT organizational structure, particularly for development and integration of close-in (less than 10 km) MASINT technologies.

In addition, the House of Representatives dealt with the management issue of MASINT legacy systems, and as a result, the Conferees to the fiscal year 2000 authorization bill directed a report, now in the hands of Congress, that addresses concerns such as the identification of collection systems, the need to review requirements, and the need to overcome operational shortfalls between national level collection and analysis and warfighter support.

Therefore, the Committee directs the Deputy Director of Central Intelligence for Community Management to conduct a utility and feasibility study to find a way to improve MASINT management and organization including the possible establishment of a centralized tasking, processing, exploitation and dissemination (TPED) facility. Of the facility options, one which should be explored is a facility located within the extended metropolitan region (less than 100 miles from nation's capital). As envisioned, such a facility would serve as a significant integration capability for specified MASINT integration cells (i.e. SURF EAGLE MASINT Integration Cell/Navy Oceanographic Command, SAR/MASINT Integration Cell/National Air Intelligence Center, the Integrated Missile-re-

lated MASINT Cell/Missile and Space Intelligence Center located in Huntsville, Alabama (see the GDIP section of the Classified Annex for details). The conceptual outline of the aforementioned study shall include management, organization and the integration facility and shall be briefed to the Intelligence Committees prior to the conference on the Intelligence Authorization Act for Fiscal Year 2001. An interim report with cost data shall be provided to the Intelligence, Appropriations, and Armed Services Committees not later than December 15, 2000. The final study shall be transmitted not later than April 1, 2001.

COUNTERTERRORISM

The Committee continues to be extremely concerned by the threat posed by international terrorism to our nation's security, and to the lives of Americans here and around the world. The Committee is further concerned that, in addition to traditional weapons such as hijacking and car bombs, terrorists' attacks are ever more likely to include chemical, biological, radiological, and nuclear weapons.

The threat of terrorist use of such weapons exacerbates an already critical threat. This threat took on crisis proportions during the recent millennium celebrations. Counterterrorism experts throughout the U.S. Government worked around the clock and resources were reportedly stretched thin. This is of particular concern given the assessment that the threat was deferred rather than defeated.

The Committee notes that all too often the United States Intelligence Community receives no thanks for its efforts. Its operations, by necessity conducted in secret, are unknown to the people whose lives are saved. The United States intelligence and law enforcement communities stand between America and terrorist plans to attack U.S. interests. The Committee has expressed its appreciation and again thanks the Intelligence Community on behalf of the American people.

The Committee will work to ensure that the Intelligence Community's efforts to fight international terrorism are well funded. In support of this goal, and because the Committee is concerned about repeated leaks of classified intelligence and the impact of these leaks on the counterterrorist effort, the Committee directs that the DCI provide a report describing any and all known leaks since January 1, 1998, that may have made the counterterrorist effort more difficult. The report should include an assessment of the potential damage to sources and methods arising from these leaks. This report should be provided to the Committee no later than December 1, 2000.

COUNTERPROLIFERATION AND ARMS CONTROL

Proliferation of chemical, biological, radiological and nuclear weapons

The Committee believes that the bi-annual reports provided by the Director of Central Intelligence pursuant to Section 721 of the Intelligence Authorization Act for Fiscal Year 1997 are valuable to the Senate and contribute to the public's knowledge of proliferation

activities of concern. The Committee also acknowledges the many classified reports and briefings on proliferation provided to the Committee and Committee Staff.

The Committee believes, however, that a number of issues warrant comprehensive assessments and in some cases, publication of unclassified separate reports.

1. Russian and Chinese proliferation to Iran

The Committee directs the DCI to provide the Committee with a comprehensive report detailing available information concerning Russian and Chinese cooperation with Iranian military programs and their transfer of sensitive technologies to Iran. This report should be provided no later than October 1, 2000, and if possible should be provided in classified and unclassified versions. The classified report should include information gained from bilateral discussions with the Russians. The unclassified version should include, to the maximum extent possible, declassification of information provided to the government of Russia under the classification "Secret, Release Only to Russia."

2. Biological weapons capabilities

The Committee commends the Intelligence Community on its publication of the National Intelligence Estimate (NIE) on biological weapons capabilities. However, the Committee believes that the information in this report should be provided in an unclassified form to the maximum extent possible. The Committee therefore directs the DCI to provide the Committee with an update to the NIE as well as an unclassified version of the NIE no later than October 1, 2000.

3. Possible Iraqi misuse of Oil for Food Program funds

The Committee is concerned by the lack of monitoring and verification of Iraqi purchases under the United Nations Oil For Food Program. While the United States reviews contracts prior to United Nations approval, no monitoring and verification program exists to confirm identified end uses and end users once items enter Iraq. The Committee therefore directs the DCI to provide the Committee with a report on the challenge posed by this lack of monitoring and verification, the number and nature of dual use items provided under Oil For Food contracts to date, and the contribution these dual use items could make to Iraq's chemical, biological, radiological and nuclear weapons, and missile programs. The report should be provided to the Congressional intelligence committees no later than February 28, 2001.

Foreign missile developments and the ballistic missile threat to the United States

The Senate report 105–24 accompanying the Intelligence Authorization Act for Fiscal Year 1998 directed the Intelligence Community to produce annual reports on the ballistic missile threat. The reports, due annually in March, have been provided in March 1998 and September 1999.

In July 1998, the Commission to Assess the Ballistic Missile Threat to the United States, also known as the Rumsfeld Commis-

sion, produced an independent assessment of and recommendations for improvements to Intelligence Community assessments. The Intelligence Community adopted these recommendations and the changes were reflected in the September 1999 report. The Committee applauds the more realistic approach to the ballistic missile threat and the analytical rigor of the September 1999 report, which was prepared as a National Intelligence Estimate, and which drew upon outside expertise as recommended by the Rumsfeld Commission.

The Committee is disappointed, however, that the Intelligence Community has missed the deadline for submission of this year's congressionally-mandated annual report. The Committee also notes that the requirement for an annual estimate on the "non-traditional" weapons of mass destruction threat to the United States, as detailed in the Senate report 105–24, has not been met. The Committee urges the Director of Central Intelligence to ensure that these Congressional requirements are satisfied. The Administration should also ensure that adequate funds and other resources are made available to enable timely provision of rigorous assessments to Congress and the American public.

Consolidation of Theater and Cruise Missile Analysis and Production

The Committee remains deeply concerned with the growing threat posed by ballistic and cruise missiles. On February 2, 2000, the Director of Central Intelligence testified before the Committee that the proliferation situation was "stark and worrisome." The DCI testified that "[t]ransfers of enabling technologies to countries of proliferation concern have not abated. Many states in the next ten years will find it easier to obtain weapons of mass destruction and the means to deliver them."

The Committee notes that the analysis and assessment of these weapons is spread among organizations within the Intelligence Community to such an extent that developers of our theater ballistic and cruise missile defense programs must deal with many different organizations, each employing different analytical methodologies and differing assumptions about the threat. The Committee believes that this situation often results in problems ranging from inconsistent data, duplication of effort, and poor use of resources.

Accordingly, the Committee recommends that the GDIP Program Manager consolidate all analysis and production of intelligence on foreign theater ballistic missiles (with ranges less than or equal to 3500 km, guided or unguided, and regardless of basing) within elements of the Defense Intelligence Agency. Furthermore, to allow a consistent approach to the analysis of all missile threats within a theater of operation, the Committee also recommends that the GDIP Program Manager consolidate all intelligence analysis of foreign cruise missiles, regardless of basing, within elements of the Defense Intelligence Agency.

North Korea

The Committee directs the Director of Central Intelligence to provide an all-source, comprehensive report covering the history

and status of all North Korean chemical, biological, radiological and nuclear programs and North Korean missile programs. This report should include all available information regarding assistance or cooperation received by North Korea from other countries. The Report should be provided no later than December 1, 2000.

Arms control monitoring

The Committee is aware that a number of arms control negotiations are underway regarding follow-on agreements to the Strategic Arms Reduction Treaty, the Anti-Ballistic Missile Treaty and the Biological and Toxin Weapons Convention. The Committee directs the Director of Central Intelligence to provide the Committee with a report on the Intelligence Community's ability to monitor the follow-on agreements under discussion and negotiation, and the contribution and challenges each agreement will make to the U.S. Government's understanding regarding other nations' programs in each of these areas. Key areas of uncertainty and resource requirements for monitoring should be addressed. To the extent possible, this report should be provided in classified and unclassified forms no later than December 1, 2000.

Enhanced monitoring of nuclear test explosions worldwide

Section 502 authorizes the Secretary of Defense to convey to a foreign government nuclear test explosion equipment to be installed within the sovereign territory of that government. This authority may be delegated to the Secretary of the Air Force. Conveyance, or other provision, of the monitoring equipment would be accomplished through bilateral agreements in which the nation receiving the equipment agrees to provide the United States with full and timely access both to the data collected and to the equipment for purposes of inspection and maintenance.

The goal of this arrangement is for the United States to obtain the cooperation of foreign governments in locating monitoring equipment in important sites throughout the world and to have the guarantee of full access to the data and equipment. This equipment would be installed as part of the United States Atomic Energy Detection System. The Intelligence Community has relied heavily on data from this system, which is operated by the United States Air Force, to monitor nuclear weapons tests on a worldwide basis. The agreements envisioned by Section 502 are with governments judged by the Intelligence Community to be capable of providing monitoring coverage in parts of the world of high U.S. national security concern.

These instruments must be properly maintained to achieve top performance. Moreover, as technology evolves, they must be upgraded to meet new U.S. standards. Section 502 authorizes the use of appropriated funds to maintain and upgrade the equipment that has been provided or conveyed to foreign governments under the agreements.

Section 502 would not authorize the provision of nuclear test explosion monitoring equipment to any international organization, including the Comprehensive Test Ban Organization and its International Monitoring System.

COUNTERDRUG

Section 308 waives two existing prohibitions and authorizes Executive branch agencies to contribute appropriated funds for the purpose of supporting the Counterdrug Intelligence Executive Secretariat established by the President's General Counterdrug Intelligence Plan (the Plan) on February 12, 2000. The Plan fulfills requirements contained in the Treasury and General Government Appropriations Act of 1998 (P.L. 105–61) and the Conference Report accompanying the Intelligence Authorization Act for Fiscal Year 1998. These two provisions required the Director of the Office of National Drug Control Policy to submit "a plan to improve coordination and eliminate unnecessary duplications among the counterdrug intelligence centers and counterdrug activities of the Federal Government," and to specifically report on efforts to structure the National Drug Intelligence Center to "effectively coordinate and consolidate strategic drug intelligence." The Congress had requested completion of these two tasks by February and April 1998 respectively. While disappointed by the two year delay, the Committee understands the difficulty in undertaking such a far-reaching, multi-agency review and appreciates the thoroughness of this effort and the subsequent Plan.

The Committee has and continues to place high priority on counterdrug intelligence programs. These programs provide essential support to the nation's efforts to attack the supply of illicit drugs and thereby reduce drug abuse and its devastating societal consequences in the United States. Intelligence is critical to effective source country programs, interdiction actions, and law enforcement investigations.

The Committee is encouraged by the steps outlined in the Plan. Although the initial reorganization and the implementation of action items is modest, the Plan has the potential to significantly enhance coordination among the various law enforcement and intelligence agencies that play a role in counterdrug efforts. Increased coordination should lead to better information sharing not only among Federal agencies, but also with and between state and local law enforcement entities.

In addition to the Counterdrug Intelligence Executive Secretariat, the Plan establishes the Counterdrug Intelligence Coordinating Group as a sub-cabinet level interagency body to oversee the Secretariat. The Group will be the primary forum for counterdrug intelligence policy discussions and resolution of interagency disputes. The Committee directs the co-chairs of the Counterdrug Intelligence Coordinating Group to provide annual reports concerning outstanding drug intelligence issues to the appropriate committees of Congress, including the Committees on Intelligence and Appropriations.

One area of concern is the lack of a permanent staff for the Counterdrug Intelligence Executive Secretariat. As currently structured, the staff will be comprised entirely of individuals on loan from other agencies. The Committee understands the valuable role that detailees can play in an interagency organization such as this, but also considers it important to maintain some number of senior staff who can provide continuity and corporate memory. The Plan

addresses this question and calls on the Counterdrug Intelligence Coordinating Group to annually review and recommend the appropriate mix of detailees and permanent staff. The Committee requests that the co-chairs of the Counterdrug Intelligence Coordinating Group inform the Committee of that recommendation.

EXPORT CONTROL

The Committee remains concerned with exports of sensitive technologies and the effect of these transfers on the capability of the Intelligence Community to collect information regarding critical threats to our nation. In recent years, the development and widespread usage of advanced computing and telecommunications systems has brought technologies previously limited to governments and militaries into the worldwide marketplace. Most of these technologies are of little or no national security significance, and pose no threat to the capabilities of intelligence agencies. Many of these technologies, however, may be used by adversaries of the United States to thwart the ability of the Intelligence Community to collect intelligence critical to our national security.

In light of these concerns, the Committee will continue to review modifications to export regulations and proposed statutory changes to existing export laws to ensure such changes do not adversely affect intelligence and national security interests.

INTELLIGENCE SHARING

The Committee maintains a keen interest in the intelligence-related implications of NATO enlargement and the subsequent evolution of European security structures. In a March 1998 report to the Senate Foreign Relations Committee, Committee staff assessed the intelligence, security, and counterintelligence implications of admitting Poland, Hungary, and the Czech Republic into NATO, noting the risks posed by these nations' past associations with Soviet intelligence services, their proximity to Russia, and continuing Russian intelligence efforts in these countries. The report also highlighted the significant steps taken by the three NATO entrants to restructure, reform, and redirect the activities of their intelligence services.

To establish a mechanism for continued monitoring of these issues, the Committee directed two reports on the procedures and methods utilized in each of the countries for the protection of intelligence sources and methods, and how these procedures and methods compared with those in place in other NATO countries. These reports have made a useful contribution to the Committee's understanding and continued oversight of these issues.

The Committee is also concerned about the implications of the evolution and proliferation of European security structures for intelligence sharing with, and within, the NATO alliance. At the recent Helsinki summit, European Union (EU) members took steps to create a European Security and Defense Identify (ESDI), but failed at the time to develop a mechanism to work with NATO on military matters. Moreover, current EU structures were not designed to manage elements such as the proposed rapid-reaction

corp nor to coordinate closer intelligence sharing among the EU members.

In addition to structural issues, as a practical matter, EU members face enormous resource challenges in making ESDI a reality, with the result that European reliance on NATO—and thus U.S.—intelligence support will remain a military reality in Europe for the foreseeable future. Many of these operational and organizational problems and shortfalls were highlighted during NATO air operations last year in the Balkans. The difficulties encountered under the relatively undemanding combat conditions over Kosovo point to far more serious difficulties that might arise in a more challenging political and military environment.

To address these and related issues, the Committee directs the DCI to provide to the Congressional intelligence committees, no later than January 1, 2001, a report in classified and unclassified form, to address the following issues:

- An update of the findings contained in the reports previously provided to the Committee concerning (a) the status and effectiveness of procedures and requirements established by Poland, Hungary and the Czech Republic for the protection of intelligence sources and methods, to include measures relating to computer, information, and communications security, and (b) an assessment of how these procedures and requirements compare with the procedures and requirements for the protection of intelligence sources and methods of other NATO members. The report should include any examples of unauthorized disclosures of U.S. or NATO classified information by any NATO member or official, or any official of a NATO member;
- The extent and adequacy of cooperation in resolving cases of espionage against the United States or NATO by U.S. citizens;
- An analysis of the NATO intelligence shortfalls and other intelligence-related lessons learned from the Kosovo campaign; and
- An analysis of the potential implications for U.S. intelligence sharing with NATO, including the protection of sources and methods, that may arise as a result of the evolution and proliferation of European security structures.

COLLECTION OF NATIONAL INTELLIGENCE

The Committee is concerned about impediments and restrictions imposed by policies, other than those directed by statute or Executive order, of any entity of the U.S. Government on the collection of national intelligence in foreign countries. The Committee notes that such policies have in some cases impeded collection of intelligence by elements of the Intelligence Community legally authorized to undertake such collection. These policies can restrict U.S. collection of high priority intelligence regarding some of the most dangerous threats to the United States. The Committee is further concerned that it was not notified of these impediments and restrictions.

The Committee therefore directs that the DCI report to the Congressional intelligence committees on all policy impediments and restrictions—written or understood—that have been interpreted to

prohibit, restrict, or discourage intelligence collection. The report should be provided to the Committees no later than 90 days after the enactment of this bill. The Committee further directs that any such impediment or restriction on the duly authorized collection of intelligence should be notified to Congress pursuant to Section 502(1) of the National Security Act of 1947, as amended.

ADMINISTRATIVE INSPECTORS GENERAL

Last year the Senate Select Committee on Intelligence reconfirmed its ongoing interest in sustaining the capabilities and independence of the administrative Inspectors General within the Intelligence Community. These include the Inspectors General at the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA).

Senate Report 106–48 called for the Directors of the above agencies to provide a written response setting out their efforts to ensure that each agency's administrative Inspector General has a separate budget line item and personnel authorization, and the authorities required to independently manage those resources. The responses to this request indicated that appropriate steps were being taken to meet these requirements. The Fiscal Year 2001 Congressional Budget Justification for each of the agencies, except the DIA, contained a separate line item for the Inspector General. The Committee also notes that the budget submission for the NIMA contained a significant budget increase for the Inspector General, giving that office greater parity with the size and capabilities of the other Intelligence Community administrative Inspectors General.

While clear progress has been made, the Committee remains concerned about the ability of the Intelligence Community's administrative Inspectors General to hire and retain staffs that are professionally and technically qualified. At some agencies, limited hiring authorities, with respect to both positions and occupations, will not allow the Inspector General to keep pace with attrition. As they seek to fill vacancies, the Inspectors General need the flexibility to hire individuals with demonstrated audit, inspection, and investigation skills, as well as individuals with expertise in critical areas such as information technology and financial and contract management. The Committee also is concerned that the relatively low government service pay for the senior managers within selected administrative Inspectors General has the potential to impair their independence, effectiveness, and credibility.

Based on these concerns, the Committee requests that the Directors of the NSA, DIA, NRO, and NIMA provide the Committee with a report outlining the projected hiring requirements of their agencies' Inspector General over the next five years. The report should include a projection of the number, qualifications, and rank of staff, as well as anticipated difficulties in acquiring or retaining these skills and positions. This report should be provided to the Committee no later than July 31, 2000.

Senate Report 106–48 also required annual reports from each administrative Inspector General detailing the fiscal and personnel resources requested for the coming fiscal year, plans for their use, comments on the office's ability to hire and retain qualified per-

sonnel, and any other concerns relating to the independence and effectiveness of the Inspector General's Office. The initial reports were helpful to the oversight process, but the Committee requests that the following information be added to future reports: a specific breakdown of staff by function (e.g. audit, inspection, investigation, or support); budget information for the two previous years, the current request, and projections for the next two years; and an overall assessment of the agency's response to the Inspector General's individual report findings and recommendations during the previous year. These reports should be provided to the Congressional intelligence committees by January 31 of each year.

RULE OF STATUTORY CONSTRUCTION

Section 305 amends the National Security Act of 1947 to add a new provision which articulates a rule of statutory construction applicable to U.S. laws enacted to implement the provisions of treaties and other international agreements. Section 305 provides that future U.S. criminal laws enacted to implement treaties shall not be construed as making unlawful what are otherwise lawful and authorized intelligence activities of the United States Government, unless Congress includes an express provision to the contrary.

United States intelligence activities currently are subject to a comprehensive regime of U.S. statutes, regulations and presidential directives that provide authorizations, restrictions and oversight. In addition, U.S. agencies involved in intelligence activities have extensive internal regulations and procedures governing appropriate levels of approval and authorization depending on the nature of such activities. These laws and regulations have developed from decades of interaction and agreement between the executive and legislative branches of the U.S. Government. The intelligence oversight committees themselves were created to meet a perceived need that the Congress must keep a close watch on the potential abuses that can occur in the intelligence area.

It is important that the Intelligence Community be able to look to this clear and precise body of U.S. domestic law, regulation and procedures as the controlling source of authority for its activities. There has been a concern that future legislation implementing international agreements could be interpreted, absent the enactment of Section 305, as restricting intelligence activities that are otherwise entirely consistent with U.S. law and policy. Of course, Congress may extend any such implementing statutes to cover intelligence activities if that is its intent, but it must do so expressly under the new provision. Such an expression of congressional intent would result in a clear prohibition that would be added to the existing body of law regulating intelligence activities. The intelligence officers who work hard to conduct lawful and authorized activities to protect the national security of the United States will not be burdened by the uncertainty that laws never intended to apply to their activities could be so interpreted.

POW/MIA ANALYSIS

Section 304 directs the Director of Central Intelligence to establish and maintain an analytic capability within the Intelligence

Community with responsibility for supporting activities related to prisoners of war and missing persons since 1990. Currently, no standing analytic capability exists. This analytical shortfall was highlighted by the case of Navy Lt. Commander Michael Speicher who was shot down over Iraq on January 17, 1991, during the Persian Gulf War. Section 943 of the National Defense Authorization Act for Fiscal Year 1998 (Public Law 105–85; 111 Stat. 1866; 10 U.S.C. 1501 note) requires the Director of Central Intelligence to provide intelligence analysis on matters concerning prisoners of war and missing persons to all departments and agencies of the Federal Government involved in such matters.

The Committee notes that Commander Speicher's fate remains unknown. The Navy declared Commander Speicher "killed in action" in May 1991. Federal regulations state that a finding of presumptive death is made when a survey of all available sources of information indicates, beyond doubt, that the presumption of continuance of life has been overcome. Information available to Congress does not necessarily support this conclusion.

The Committee has reviewed the support of the Intelligence Community for the decision of the United States Government to characterize Commander Speicher's status as "killed in action." The review was based upon a September 1998 report by the Direct or Central Intelligence and additional information on the chronology of the disappearance of Commander Speicher. The Committee concluded that it is critical that an intelligence organization be specifically assigned responsibility for analysis of all-source information on POW/MIA matters, including information derived from sensitive intelligence sources and methods, such as the information collected with respect to Commander Speicher.

The case of Commander Speicher demonstrates that valid questions about POW/MIAs remain today, and that rigorous and timely analytic assessments and accountability are essential to resolving such questions. A POW/MIA analytic capability in the Intelligence Community is required. The Committee understands the sporadic nature of the requirement for this analytic capability and directs the DCI to designate a small number of analysts with responsibility for current POW/MIA issues and with the capability to surge their effort should the need arise.

NATIONAL FOREIGN INTELLIGENCE PROGRAM

Guidelines and limitations governing intelligence collection information on U.S. persons

The Committee is concerned about recent media accounts alleging that the National Security Agency (NSA) conducts activities that may violate the constitutional rights of United States persons.

The NSA's primary mission is to intercept and analyze the communications of foreign adversaries, including terrorists and drug traffickers. The President and other policymakers rely heavily on the critical information provided by the NSA. The Committee recognizes the potential intrusion into the private lives of U.S. citizens inherent in this type of intelligence collection, and the need to remain vigilant to ensure that the laws and regulations that protect the privacy of U.S. persons are strictly adhered to. This Committee

was created in part in response to violations of the constitutional rights of American citizens by intelligence agencies that at times lost sight of the critical balance between defending national security and defending those values upon which our security as a nation ultimately depends. The Committee has no more critical responsibility than to ensure that this balance is maintained.

In the 1970's, after congressional inquiries revealed abuses by the NSA, CIA and FBI, the Congress and the Executive branch created an extensive structure of laws and oversight (including the creation of the Congressional oversight committees). These laws, executive orders and regulations established stringent guidelines and limitations governing the collection of information on U.S. persons. Finally, the intelligence agencies, including the NSA, were prohibited by presidential executive order from circumventing United States legal restrictions by asking foreign agents or governments to collect information on their behalf.

The Committee believes, based on all available information, that the NSA is in compliance with applicable laws and regulations. The NSA is required by law to keep the oversight committees fully and currently informed of all significant intelligence activities and must report any illegal intelligence activities. Moreover, the NSA, in coordination with the CIA and the Justice Department, was required last year by Congress to conduct a review of the legal standards in place to protect the constitutional rights of U.S. persons from intrusive electronic surveillance. The report indicates that the legal standards controlling the NSA's electronic surveillance are effective in adhering to the requirements of the Fourth Amendment to the United States Constitution. As noted above, however, the Committee has no more critical responsibility than to ensure that the balance between national security and rights of Americans established in law is maintained, and will continue to monitor strictly the NSA's activities.

Experimental Personnel Management Program for Technical Personnel for Certain Elements of the Intelligence Community

Section 503 establishes an experimental personnel program providing the Director of Central Intelligence with limited authority over a five-year period to recruit up to 39 science and engineering experts for advanced research and development projects administered by three elements of the Intelligence Community. Of the 39 positions covered under this personnel program, the National Imagery and Mapping Agency (NIMA) will be allocated no more than fifteen positions, the National Security Agency twelve positions, the National Reconnaissance Office six positions, and the Defense Intelligence Agency six positions. Expanded hiring authorities of this type were granted to the Defense Advanced Research Projects Agency in fiscal year 1999. The need for such authorities in the Intelligence Community has been supported by the testimony of the respective program managers and was reaffirmed by the Committee's May 1999 Technical Advisory Group report on the NIMA, the future of imagery intelligence, and the emerging challenge of modernizing the Intelligence Community's tasking, processing, exploitation, and dissemination system.

Beginning in 2001, the DCI must submit, no later than October 15 of each year in which employees serve under the program, an annual report to the intelligence oversight committees of the Congress. The annual report shall include a discussion on the DCI's exercise of the special personnel management authority during the reporting period, the sources from which individuals appointed were recruited, and the methodology of identification and selection of recruits.

Functional management of Tactical Imagery and Geospatial Programs

The Committee is concerned that the National Imagery and Mapping Agency (NIMA) does not exercise comprehensive functional management authority over U.S. imagery and geospatial programs. The NIMA's founding legislation, Public Law 104–201, sets forth authorities provided to the NIMA Director in relation to other elements of the Intelligence Community, the Department of Defense, and the military services. Department of Defense Directive Number 5105.60 established the NIMA within the Defense Department and prescribed its mission, organization, responsibilities, and authorities. Department of Defense Directive Number 5105.60 notes two types of management authority those of a functional manager and those of a program manager. Functional management is defined as "[t]he review of and coordination on investment activities related to imagery, imagery intelligence, and geospatial information, which includes RDT&E [research, development, testing, and evaluation] and procurement activities within the NFIP (National Foreign Intelligence Program), JMIP (Joint Military Intelligence Program), and TIARA (Tactical Intelligence and Related Activities) aggregate." Although not defined, program management authority is understood in practice to include the authority to make program investment decisions as well as all authorities present under functional management.

The NIMA's authorities regarding national and tactical level imagery, imagery intelligence, and geospatial programs are different for each function. The NIMA Director is both "program manager" and "functional manager" for the National Imagery and Mapping Program within the NFIP and the Defense Imagery and Mapping Program within the JMIP. As such, the NIMA Director is tasked with providing imagery, imagery intelligence, and geospatial information for national customers within the CIA, the State Department, the Office of the Secretary of Defense, and the service components, and has the authority to make program investment decisions to support these missions.

However, the NIMA Director serves only as the "functional manager for imagery, imagery intelligence, and geospatial investment activities which include Research, Development, Testing and Evaluation (RDT&E) and procurement initiatives within the Tactical Intelligence and Related Activities (TIARA) aggregate." As a result, the NIMA Director has less influence over the tactical imagery and geospatial programs within the military services.

The National Defense Authorization Act (P.L. 104–201) amended the National Security Act of 1947 (50 U.S.C. 403–5(b)) to provide the NIMA with substantial functional management authority.

Under the amended section 105(b)(2) of the National Security Act, the NIMA Director is responsible, "notwithstanding any other provision of law, for prescribing technical architecture and standards related to imagery intelligence and geospatial information and ensuring compliance with such architecture and standards." This provision was further expanded by Department of Defense Directive 5105.60, which provides the NIMA with the authority to set standards for end-to-end architecture related to imagery, imagery intelligence, and geospatial information; geospatial information products; career and training programs for imagery analysts, cartographers, and related fields; and technical guidance regarding standardization and interoperability for systems utilizing imagery, imagery intelligence, and geospatial information.

Officials involved in the formation of the NIMA believed the combination of authority to set standards, and review investment and RDT&E decisions, would provide the NIMA with a significant ability to influence tactical imagery and geospatial programs even though the agency did not control their funding. However, current NIMA officials have commented that the authority merely to review investment and RDT&E decisions has not given the NIMA a prominent position in the budget review process. Being a relatively new agency, the NIMA has had to work to assert its role in the already established Department of Defense and Intelligence Community infrastructures.

To address a similar lack of comprehensive management with regard to tactical signals intelligence programs, the Deputy Secretary of Defense in 1995 granted the National Security Agency Director approval authority over the tactical investment and RDT&E decisions of the Defense Cryptologic Programs of the service components. National Security Agency (NSA) officials have stated that this approval authority enabled the NSA Director to be more involved in investment and RDT&E decisions earlier in the budget process, thereby assuring that his recommendations and guidance as functional manager of signals programs were incorporated into tactical systems.

In September 1999, the Committee issued an audit report of the NIMA's structure, mission, and role within the Intelligence Community. The first conclusion of the audit report is that the lack of approval authority over tactical investment and RDT&E programs limits the ability of the NIMA Director to serve as the functional manager for imagery and geospatial programs. The NIMA has had difficulty receiving information about tactical programs in a timely manner and has had to provide its recommendations on service components plans late in the budget review process. The Committee recommended that the Secretary of Defense grant the NIMA Director the approval authority over service component imagery and geospatial investment and RDT&E programs to ensure that NIMA has an established role and can provide oversight early in the budget process.

The recently completed Defense Science Board Task Force report on NIMA concurred with the Committee's recommendation:

> **"RECOMMENDATION 1: Strengthen NIMA's Role as Functional Manager of U.S. Imagery and Geospatial Information** "* * * The Deputy Secretary of

> Defense and the Director of Central Intelligence (DCI) need to reemphasize NIMA's charter as the executive agency for all geospatial information, much as NSA is the executive agency for all SIGINT information."

The Secretary of Defense, in his January 5, 2000, reply to the Committee's audit report concurred with all of its conclusions and recommendations and noted that his staff was working with the NIMA on implementing them, with the exception of the recommendation to grant the NIMA approval authority over tactical investment and RDT&E decisions. The reply states: "We are currently working with the Services and with NIMA to evaluate this recommendation, and we hope to reach a decision within the next few months." To date, no such decision has been reached.

The Committee reiterates its support for strengthening the role of the NIMA Director as functional manager of U.S. imagery and geospatial programs and directs the Secretary of Defense to provide a status report on efforts to implement the recommendations pertaining to this issue contained in the Committee and Defense Science Board Task Force reports. The report shall be submitted to the Committee no later than July 31, 2000.

Hard Copy Production in the Future Imagery Architecture (FIA) Era

The National Reconnaissance Office (NRO) has no stated requirement to generate hard copy products for the Intelligence Community as part of the Future Imagery Architecture (FIA), nor does the National Imagery and Mapping Agency (NIMA) plan to produce these products. The Committee is concerned that the transition to soft copy image display and archiving systems has been slower than planned, potentially creating a situation where current hard copy imagery users will not be able to receive soft copy images when the FIA becomes operational. Therefore, the Committee directs the Director of the NIMA, in coordination with the Director of the NRO, to provide a report detailing imagery user requirements and a roadmap for the transition of hard copy imagery users to soft copy before the FIA begins operation. The report shall be submitted to the Congressional intelligence committees no later than July 31, 2000.

Critical Intent Model 2 (CIM2)

Given the emergence of new and ambiguous threats, it is important for the United States, its allies and future coalition partners to find and develop additional ways to exploit new information technology to improve radically their crisis avoidance, situation assessment, and collaboration capabilities. The explosion of information available combined with reduced resources available for national security programs highlighted the need for a fast and efficient capability to detect and manage crises. The Committee is aware of the Critical Intent Model (CIM)—a structured argumentation tool—as a key enabling technology in PROJECT GENOA, which provides analysts and policy makers with the capability to track ongoing and evolving situations, collect analysis, and enable users to discover previously unknown information and critical data relationships. The CIM structured argumentation tool facilitates

more comprehensive analysis, creates a corporate memory for use in current analysis, and allows the comparison and contrasting of details of a particular argument. Moreover, CIM captures logic patterns for policy option analysis and serves as a foundation for scenario-based crisis avoidance systems.

The Committee recommends the transition of the CIM structured argument prototype software from the Defense Advanced Research Projects Agency to the Intelligence Community, and strongly recommends investment by the Intelligence Community in the CIM structured argument tool with available fiscal year 2000 and 2001 funds.

Funding of intelligence activities, section 504

At a time when the Intelligence Community faces many difficult decisions about spending priorities, the Committee continues to be concerned that the budget practices of the CIA and the Intelligence Community as a whole are simply inadequate to address current requirements. Upper level program managers lack sufficient insight into the process to make informed and timely decisions regarding the allocation of funds, and to assure Congress, and themselves, that funds are being spent as appropriated and authorized. The Committee is particularly troubled by recent CIA reprogramming requests that appear not to meet legal requirements.

Those legal requirements are outlined in Section 504 [50 U.S.C. 414] of the National Security Act of 1947. According to Section 504, "[a]ppropriated funds available to an intelligence agency may be obligated or expended for an intelligence or intelligence-related activity only if:

> (1) those funds were specifically authorized by the Congress for use for such activities; or
>
> (2) in the case of funds from the Reserve for Contingencies * * * or
>
> (3) in the case of funds specifically authorized by Congress for a different activity—
>
> > (A) the activity to be funded is a *higher priority* intelligence or intelligence-related activity;
> >
> > (B) the need for funds for such activity is based on *unforseen requirements;* and
> >
> > (C) the Director of Central Intelligence, * * * has *notified the appropriate congressional commitees* of the intent to make such funds available for such activity * * *" (emphasis added).

In the case of the CIA, the Committee is not convinced that all funds reprogrammed in fiscal year 2000 met the thresholds of "higher priority" and "unforseen requirements" as stated in the National Security Act of 1947. Recent actions, including taxing directorates for funds to be used in other areas, and moving funds within expenditure centers without Congressional notification, have eroded this Committee's confidence that appropriations are used as intended. The Committee understands that the CIA's Inspector General is conducting an audit of the CIA's budget process and reprogramming practices and will report on the overall budget process and compliance with Section 504. Such an independent and de-

tailed assessment is long overdue, and we applaud the Inspector General's efforts in this regard.

To address the Committee's concern that resources be obligated and expended as intended by Congress, without unduly restricting the CIA's flexibility to respond to high-priority unfunded requirements, the Committee directs the CIA's Comptroller to provide to the Congressional intelligence committees quarterly briefings on the CIA's execution of its budget during the remainder of fiscal year 2000 and in fiscal year 2001. These briefings should provide the committees with sufficient information to demonstrate the CIA's compliance with Section 504.

Joint Signals Intelligence (SIGINT) Avionics Family

The proposed fiscal year 2001 budget includes $17.0 million in Air Force procurement funding for the purchase of one Joint SIGINT Avionics Family (JSAF) High Band Subsystem (HBSS)/ Low Band Subsystem (LBSS) unit. The proposed funding is insufficient to purchase the appropriate spares, aircraft cabling, antennas, and installation needed to field the first operational JSAF system on the U–2 aircraft. The current JSAF procurement plan is to procure one U–2 JSAF unit in fiscal year 2002 and two JSAF units in each of the next five years. This funding plan fails to take advantage of economics of scale associated with higher production rates, delays fielding the JSAF capability in the U–2 fleet, and will not support the stated goal of maintaining 11 sensors (a combination of RAS–1R and JSAF) by the end of 2004 when aircraft currently in the fleet will no longer be flown. The Air Force deploys the U–2 aircraft in detachments of three planes to their forward operating bases, and the current requirement is to have no fewer than two of the three aircraft carrying the JSAF.

Therefore, the Committee recommends an addition of $52.0 million in Air Force procurement funding to the JSAF program: (1) $8.0 million to fully fund the first JSAF unit with appropriate antennas, spares and installation on the U–2; and (2) $44.0 million to procure two additional units to take advantage of economies of scale and to provide sufficient units for fielding a complete detachment of three U–2 aircraft.

Geospatial Production

The National Imagery and Mapping Agency (NIMA) is in the initial stages of an internal reorganization and realignment of personnel that will shift almost one-tenth of its geospatial workforce over to imagery analysis to better meet the growing needs of the imagery customer base. Over the five years, beginning in fiscal year 2001, a total of 300 geospatial experts—60 positions a year—will be retrained as imagery analysts. As a result, geospatial production readiness within the Intelligence Community will degrade and the NIMA's reliance on the contractor community for the outsourcing of geospatial products will increase. The Committee recommends an additional $5.0 million for geospatial production under the NIMA's Omnibus Outsourcing Program to shore up this erosion in readiness.

TACTICAL INTELLIGENCE AND RELATED ACTIVITIES

GUARDRAIL Common Sensor

The GUARDRAIL Common Sensor (GRCS) is a corps-level, airborne signals intelligence collection and location system capable of providing tactical commanders with near-real time targeting information. The GRCS combines communications intelligence and electronic intelligence capabilities onboard multiple versions of RC–12 fixed-wing aircraft.

The Committee recommends an addition of $2.0 million in Army procurement funding for the GUARDRAIL modifications effort to accelerate the integration of the Tactical Intelligence Broadcast System (TIBS) capability for GRCS System 2. The additional funding will complete the integration of TIBS in the last of four GRCS systems.

Joint Surveillance Target Attack Radar System Common Ground System

The Common Ground System receives, processes, correlates, and disseminates data simultaneously from the Joint Surveillance Target Attack Radar System, unmanned aerial vehicles, and other tactical, theater and national systems for targeting, situation development, and battle management.

The Committee recommends a reduction of $2.0 million in Army RDT&E funding proposed for the Distributed Common Ground Station—Army prototype. The Committee understands that this effort duplicates an effort being performed under the Army's Tactical Exploitation of National Capabilities program.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of 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 2001 and lists authorization of appropriations for conduct of intelligence and intelligence activities for certain elements of the United States Government for fiscal years 2002 through 2005.

Section 102. Classified Schedule of Authorizations

Section 102 states 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 2001 are contained in a classified Schedule of Authorizations. The Schedule of Authorizations is incorporated into the Act by this section.

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, in fiscal year 2001 to exceed 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 ceil-

ings 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 intelligence oversight committees of the Congress.

Section 104. Community Management Account

Section 104 provides 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 $232,051,000 for fiscal year 2001 for the staffing and administration of various components under the CMA. Subsection (a) also authorizes funds identified for the Advanced Research and Development Committee to remain available for two years.

Subsection (b) authorizes a total of 618 full-time personnel for elements within the CMA for fiscal year 2001 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 (e) requires the Director of Central Intelligence to transfer the $27,000,000 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.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of Appropriations

Section 201 authorizes appropriations in the amount of $216,000,000 for fiscal year 2001 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL PROVISIONS

Section 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.

Section 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.

Section 303. Prohibition on Unauthorized Disclosure of Classified Information

Section 303 creates a basis in law for prosecuting the knowing and willful unauthorized disclosure of classified information to a person not authorized to receive that information. This section closes the gap in existing law for the unauthorized disclosure of classified information.

Section 304. POW/MIA Analytic Capability in the Intelligence Community

Section 304 requires the Director of Central Intelligence to establish and maintain a POW/MIA analytic capability within the Intelligence Community with responsibility for intelligence in support of the activities of the United States relating to prisoners of war and missing persons.

Section 305. Applicability to Lawful United States Intelligence Activities of Federal Laws Implementing International Treaties and Agreements

Section 305 amends the National Security Act of 1947 to add a new provision which articulates a rule of statutory construction applicable to U.S. laws enacted to implement the provisions of treaties and other international agreements. Section 305 provides that future U.S. laws enacted to implement treaties shall not be construed as making unlawful what are otherwise lawful and authorized intelligence activities of the United States, unless Congress includes an express provision to the contrary.

Section 306. Limitation on Handling, Retention, and Storage of Certain Classified Materials by the Department of State

Section 306 requires the Director of Central Intelligence to certify to Congress that each element of the Department of State that handles, retains or stores material classified at the Sensitive Compartmented Information (SCI) level is in full compliance with all applicable Director of Central Intelligence directives (DCIDs) or Executive Orders regarding the handling, retention, or storage of SCI materials. As of January 2001, funds authorized to be appropriated under this Act for the Department of State Bureau of Intelligence and Research shall be prohibited from obligation or expenditure so long as any covered element of the Department of State has not been certified by the Director of Central Intelligence (DCI) as being in full compliance. Any element of the Department of State not certified will be prohibited from retaining or storing material classified at the SCI level until the DCI certifies its compliance, unless such elements receive a Presidential waiver.

Section 307. Clarification of Standing of United States Citizens to Challenge Certain Blocking of Assets

Section 307 amends the Foreign Narcotics Kingpin Designation Act (title VIII of Public Law 106–120) (hereafter referred to as the "Act"). This provision simply states that whatever process was available to a United States citizen under the Administrative Procedure Act or any other provision of law, with respect to the blocking of assets by the United States, prior to the enactment of the

Act, remains available after the enactment of the Act. It was not the intent of the United States Congress to abrogate in any way the due process rights of U.S. citizens upon the enactment into law of the Foreign Narcotics Kingpin Designation Act. Section 307 expressly states in statutory language Congress's original intent.

Section 308. Availability of Certain Funds for Administrative Costs of Counterdrug Intelligence Executive Secretariat

Section 308 waives prohibitions that prevent Executive branch agencies from contributing appropriated fiscal year 2000 funds to an interagency body for the purpose of supporting the Counterdrug Intelligence Executive Secretariat.

TITLE IV—CENTRAL INTELLIGENCE AGENCY

Section 401. Expansion of Inspector General Actions Requiring a Report to Congress

Section 401 closes gaps in the reporting requirements to the intelligence oversight committees of the Congress revealed by the Committee's inquiry into the mishandling of classified information by former DCI John Deutch. Current law requires the Inspector General to notify the intelligence oversight committees only if the Director or Acting Director is the subject of an inquiry. This amendment broadens the notification requirement to include former DCIs, all confirmed officials (General Counsel, DDCIs and ADCIs), the Executive Director, and the Deputy Directors for Operations, Intelligence, Administration, and Science and Technology. In addition to expanding the number of senior officials covered by the notification requirement, the amendment also requires congressional notification whenever a criminal referral to the Department of Justice is made on one of the designated officials.

Section 402. Subpoena Authority of the Inspector General of the Central Intelligence Agency

Section 402 provides several technical corrections to the Central Intelligence Agency Act of 1949 to address superseding legislation, conform language and streamline reporting procedures.

Section 403. Improvement and Extension of Central Services Program

Section 403 extends the Central Services Program until March 31, 2005, and clarifies that the Central Services Program Working Capital Fund may retain and use receipts resulting from reimbursements for utility services and meals provided to individuals and cash receipts from the rental of property and equipment to employees and detailees. This change would allow the Central Services Program Working Capital Fund to retain miscellaneous receipts that are paid directly to an enterprise by an individual, thereby properly offsetting costs incurred in the operation and maintenance of enterprise facilities where the Government incurs costs associated with those individuals. In addition, this section expands the current law to allow retention of rents collected from individuals who are not CIA employees, and therefore not subject to

payroll deduction. Finally, this section excludes depreciation of CIA owned structures as a recoverable operating expense.

Section 404. Details of Employees to the National Reconnaissance Office

Section 404 amends the Central Intelligence Agency Act to permit the Director of Central Intelligence to detail CIA employees on a long-term basis to the National Reconnaissance Organization (NRO). Current laws, regulations and Comptroller General opinions which govern the detailing of employees from one government agency to another have been interpreted by the CIA General Counsel to limit details to NRO to no more than five years. This amendment would exempt CIA from these requirements and would provide the flexibility necessary to deal with the unique staffing requirements of the NRO.

Section 405. Transfers of Funds to Other Agencies for Acquisition of Land

Section 405 extends the life of appropriated funds transferred by the CIA permitting them to remain available for three years to other government agencies for the purpose of purchasing land. Any exercise of this authority must be reported to the intelligence oversight committees of the Congress.

Section 406. Eligibility of Additional Employees for Reimbursement for Professional Liability Insurance

Section 406 allows the Director of Central Intelligence to designate categories of employees in addition to those noted in Public Law 104–208, who would be eligible to receive reimbursement for up to one-half of the cost of purchasing professional liability insurance. This section permits the expenditure of appropriated funds to reimburse employees who are at risk of incurring liability claims due to the nature of their duties, but are not included within the existing job categories that are currently eligible for reimbursement. Any exercise of this authority must be reported to the intelligence oversight committees of the Congress.

TITLE V—DEPARTMENT OF DEFENSE INTELLIGENCE ACTIVITIES

Section 501. Two-year Extension of Authority to Engage in Commercial Activities as Security for Intelligence Collection Activities

Section 501 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, 2002. This authority expires on December 31, 2000.

Section 502. Nuclear Test Monitoring Equipment

Section 502 authorizes the Secretary of Defense, who may delegate the authority to the Secretary of the Air Force, to convey to a foreign government nuclear test explosion monitoring equipment that is installed within the territory of that government. This equipment would be conveyed with a bilateral agreement in which the recipient nation agrees to provide the United States with timely access to the data produced, collected, or generated and to pro-

vide the U.S. access to the equipment for purposes of inspecting, testing, maintaining, repairing, or replacing the equipment.

Section 503. Experimental Personnel Management Program for Technical Personnel for Certain Elements of the Intelligence Community

Section 503 allows the Director of Central Intelligence (DCI), for a period of five years from the date of enactment of this Act, to carry out an experimental program using special personnel management authority to facilitate the recruitment of eminent experts in science or engineering for research and development projects administered by the National Imagery and Mapping Agency (NIMA), the National Security Agency (NSA), the National Reconnaissance Organization (NRO), and the Defense Intelligence Agency (DIA). Under this limited authority, the DCI may appoint scientists and engineers from outside the civil service and uniformed services to the NIMA, NSA, NRO and DIA.

COMMITTEE ACTION

On April 27, 2000, the Select Committee on Intelligence approved the Bill and ordered that it be favorably reported. The Committee approved by a vote of 12–1 an amendment by Senator Levin to add Section 307, a clarification of the standing of United States citizens to challenge certain blocking of assets by the United States.

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 2001, 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 May 4, 2000, the Committee transmitted this Bill to the Congressional Budget Office (CBO) 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) 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.

○