AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

107TH CONGRESS
1st Session

SENATE

REPORT
107–51

COMMITTEE ACTIVITIES

SPECIAL REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE
JANUARY 6, 1999 TO DECEMBER 15, 2000

AUGUST 3, 2001.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
89–010 WASHINGTON : 2001

CONTENTS

	Page
I. Introduction	1
II. Legislation	3
A. Intelligence Budget	3
B. S. 1009 Intelligence Authorization Act for FY 2000	3
C. S. 2507 Intelligence Authorization Act for FY 2001	5
D. S. 2089, The Counterintelligence Reform Act for FY 2000	6
E. S. 1902 Japanese Imperial Government Disclosure Act of 2000	7
III. Oversight Activities	8
A. Hearings	8
1. Counterintelligence	8
2. Counterterrorism	8
3. Counterproliferation	9
4. Counternarcotics	10
5. Denial and Deception	11
6. Ballistic Missile Analysis	11
7. State Department Security Breaches	11
8. National Security Threats to the U.S.	13
9. Covert Action Quarterly Reviews	14
10. Kosovo	14
11. Russia	15
12. The People's Republic of China (PRC)	16
13. Colombia	16
14. Iraq	16
15. India/Pakistan	17
16. Cyber Security	17
17. Y2K	18
18. Lt. Commander Michael Speicher	18
19. Nazi War Crimes	20
20. Encryption	20
21. CTBT	21
22. FISA and the Technology Challenge	21
23. Pan Am 103	22
24. Intelligence Needs of Unified Commanders	22
25. NIMA/TPED	23
26. Unauthorized Disclosure of Classified Information	24
B. Investigations and Inquiries	25
1. China Investigations	25
2. PRC Nuclear Espionage, Department of Energy Security and Counterintelligence Matters, and the Wen Ho Lee Case	30
3. Deutch Mishandling of Classified Material	31
4. USS *Cole*	32
C. Community Issues	33
1. Activities of the CIA in Chile	33
2. Oversight of Intelligence Community Inspectors General	33
3. Classified Information Procedures Act (CIPA)	34
4. POW/MIA Analytic Capability in the Intelligence Community	35
5. Counterdrug Intelligence Plan	36
6. Judicial Review Commission on Foreign Asset Control	36
7. National Commission for the Review of the National Reconnaissance Office	37
D. Audits	37
1. NIMA	38
2. Covert Action	38
3. Other	38
E. Technical Advisory Group (TAG) Reports	38
1. Signals Intelligence—Rebuilding the NSA	39
2. Human Intelligence—Bringing Technology in from the Cold	40

Page

3. MASINT—Funding and Organizing to Realize Potential 41
4. IMINT—Keeping the Customers Satisfied 41

IV. Confirmations 42
A. James M. Simon, Jr., Assistant Director of Central Intelligence for Administration 42
B. John McLaughlin, Deputy Director of Central Intelligence 42

V. Support to the Senate 42

VI. Appendix 43
A. Summary of Committee Activities 43
1. Number of Meetings 43
2. Bills and Resolutions Originated by the Committee 43
3. Bills Referred to the Committee 43
4. Publications 43

107TH CONGRESS
1st Session

SENATE

REPORT
107–51

COMMITTEE ACTIVITIES—SPECIAL REPORT OF THE SELECT COMMITTEE ON INTELLIGENCE, UNITED STATES SENATE, JANUARY 6, 1999 TO DECEMBER 15, 2000

AUGUST 3, 2001.—Ordered to be printed

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

SPECIAL REPORT

I. INTRODUCTION

The Senate Select Committee on Intelligence (SSCI) was established in 1976 by Senate Resolution 400 to strengthen Congressional oversight of the programs and activities of U.S. intelligence agencies. Throughout its history, the Committee has sought to carry out its oversight responsibilities in a nonpartisan manner. During the 106th Congress, the Committee continued this tradition in crafting important intelligence legislation, conducting investigations and audits into Intelligence Community and other national security issues, and authorizing and as necessary, increasing or reallocating—funding for a wide array of U.S. intelligence activities.

As part of its oversight responsibilities, the Committee performs an annual review of the intelligence budget submitted by the President and prepares legislation authorizing appropriations for the various civilian and military agencies and departments comprising the Intelligence Community. These entities include the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, National Imagery and Mapping Agency, National Reconnaissance Office, as well as the intelligence-related components of Department of State, Federal Bureau of Investigation, Department of the Treasury, and Department of Energy. The Committee makes recommendations to the Senate Armed Services Committee on authorizations for the intelligence-related components of the U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine Corps. The Committee also conducts periodic investigations, audits, and inspections of intelligence activities and programs.

The Committee's charge is to ensure that the Intelligence Committee provides the accurate and timely intelligence necessary to identify and monitor threats to the national security to support the executive and legislative branches in their decisions on national se-

curity matters, ensure that U.S. military commanders have the intelligence support to allow them to prevail swiftly and decisively on the battlefield, and to ensure that all intelligence activities and programs conform with the Constitution and laws of the United States of America.

Following the dissolution of the Warsaw Pact and the Soviet Union, the U.S. Intelligence Community has reviewed, redirected, and expanded its efforts to monitor both traditional and emerging national security threats, including so-called "asymmetric threats," confronting the United States. The emergence and growth of transnational threats such as the proliferation of weapons of mass destruction, international terrorism, information warfare, narcotics trafficking, and international criminal organizations presents the nation and the Intelligence Community with challenges requiring different policies, programs, technologies, and structures. These challenges are compounded by dramatic advances in telecommunications technology, including the spread of strong encryption, and the growth of foreign denial and deception activities designed to conceal, or mislead as to, activities of concern to U.S. intelligence collectors, analysts, and policymakers. As new challenges and threats confront the country, the Committee plays an ever more important role in ensuring that the Intelligence Community adapts to and meets these evolving threats and intelligence challenges.

The need to modernize the Intelligence Community's infrastructure—both "hardware" (e.g., collection, communications, dissemination, and support systems) and "human software" (e.g. leadership, motivation, innovation, language skills, and analysis) with which the Community approaches the future—was a central theme of the Committee's work in the 106th Congress. As in the 105th Congress, the Committee built upon the work of the SSCI Technical Advisory Group (TAG) in identifying problems, solutions, and opportunities for Committee action.

Reflecting the recommendations of the TAG as well as other problems and shortfalls identified by the Committee, the Committee in the 106th Congress has continued to fight, with some success, to increase the overall level of intelligence spending above the President's budget request, while reducing or reallocating funds from programs and activities that were poorly justified, redundant or lower in priority. The Committee sought to focus on the most imminent and critical challenges facing the Intelligence Community, including an aging U.S. signals intelligence (SIGINT) collection system, and serious shortfalls in the Tasking, Processing, Exploitation, and Dissemination (TPED) of intelligence from satellites and other collection platforms. In addition, the Committee continued to concentrate additional resources and attention on the five areas of counternarcotics, counterterrorism counterproliferation, counterintelligence, and effective covert action.

The Committee focused special oversight and legislative attention on counterintelligence and security matters, including The People's Republic of China (PRC) nuclear espionage and a series of security problems at the Department of State. In addition to its investigation into PRC espionage and security problems at the Department of Energy, the Committee conducted extensive investigations into satellite and missile technology transfers to the PRC, the PRC efforts to influence U.S. policy, and the mishandling of highly

classified information by former Director of Central Intelligence John Deutch. The Committee also adopted a provision—later vetoed by President Clinton—to deter leaks of classified information.

During the 106th Congress, the Committee conducted 99 hearings and on-the-record meetings. Of these, 57 were oversight hearings, 12 were budget hearings (including conference meetings with the House committee), 20 were legislative hearings, eight were business meetings, and two were nomination hearings. The Committee also held 17 on-the-record briefings and more than 250 off-the-record briefings.

II. LEGISLATION

A. INTELLIGENCE BUDGET

The Committee conducted annual reviews of the fiscal year 2000 and fiscal year 2001 budget requests for the Director of Central Intelligence's National Foreign Intelligence Program (NFIP), and the Department of Defense's Joint Military Intelligence Program (JMIP) and Tactical Intelligence and Related Activities (TIARA). As part of its review, the Committee received testimony from senior Intelligence Community officials and evaluated the detailed budget justification documents submitted by the executive branch.

The Committee is concerned that for a number of years, the funding allocated for intelligence activities has been inadequate. While some reallocation of national resources was inevitable after the end of the Cold War, the Committee believes the time has come to increase funding for intelligence activities to ensure timely and adequate warning of threats to our national security in a complex and challenging security environment. The Committee identified substantial shortfalls in modernization programs for some agencies that can only be addressed by additional resources, or a realignment of priorities for intelligence expenditures.

The Committee also has recommended a five year realignment of resources for fiscal years 2001–2005, should the executive branch choose not to increase the allocation of resources for intelligence.

During the 106th Congress, the Committee maintained its commitment to advanced research and development efforts community-wide and strengthening U.S. capabilities in the areas of counterproliferation, counterterrorism, counternarcotics, counterintelligence and covert action.

B. S. 1009, FY 2000 INTELLIGENCE AUTHORIZATION ACT

On May 11, 1999, the Committee reported S. 1009, the Intelligence Authorization Bill for Fiscal Year 2000. The bill provided the annual authorization for appropriations for intelligence activities and included several legislative provisions. Some of these provisions:

Authorized the intelligence activities and programs for the Central Intelligence Agency (CIA), the Department of Defense (DOD), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the Department of the Army, the Department of the Navy, the Department of the Air Force, the Department of State, the Department of the Treasury, the Department of Energy (DOE), the Federal Bureau of Investiga-

tion (FBI), the National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA).

Authorized investigative components, such as the Federal Bureau of Investigation (FBI) and internal Intelligence Community investigative or security elements, to access computers of individuals handling classified data, with the consent of the individual.

Expanded the definition of "agent of a foreign power" under the Foreign Intelligence Surveillance Act (FISA) to include the classic illegal spy who comes to the United States under a false identity and remains hidden for many years before being tasked to conduct espionage.

Expanded the discretion available to government officials under the Immigration and Nationality Act to permit naturalization of persons who have made an extraordinary contribution to the national intelligence mission and who were otherwise disqualified because of past membership in the Communist Party or other totalitarian organization.

On the floor, the Senate took up the intelligence authorization bill passed by the House and struck all of the House bill after the enacting clause and inserted a substitute text, consisting of the text of S. 1009 and amendments. In conference, members of the House Permanent Select Committee on Intelligence (HPSCI) and the SSCI met to seek agreement on the authorization of appropriations for fiscal year 2000 and to resolve differences in the legislative provisions in the House and Senate bills. The HPSCI receded from its disagreement to the amendment of the Senate with an amendment that was a substitute for the House bill and the Senate amendment. The conference report passed both houses and was signed by the President on December 31, 1999, as P.L. 106–120. The provisions of S. 1009 described above remained in the final conference report. In addition, the conference report:

Established procedures for blocking assets of foreign narcotics traffickers who pose an unusual and extraordinary threat to national security (the "Foreign Narcotics Kingpin Designation Act") and created a Judicial Review Commission to evaluate and report on remedies available to U.S. persons affected by the blocking of assets of foreign persons.

Required a declassification review and critical analysis of an intelligence estimate on Vietnam-era personnel who are listed as prisoners-of-war or missing-in-action personnel (POW/MIA).

Established the Commission for the Review of the National Reconnaissance Office (NRO) tasked with reviewing the roles and missions of the NRO to ensure that the Intelligence Community acquires the most efficient technologically capable, and economical satellite collection systems.

The Foreign Narcotics Kingpin Designation Act was added to the Senate bill as an amendment during floor consideration. The conferees debated at length the issue of the judicial review available to U.S. persons whose assets may be affected by the blocking of assets of foreign drug kingpins. The conferees agreed to appoint a Judicial Review Commission to study whether adequate judicial review was available and report back to the Committees.

The POW/MIA provision in the conference report was a floor amendment to the Senate bill and was accepted by the managers.

The NRO Commission provision was added at conference. The managers agreed that the functions and missions carried out by the NRO are essential to the provision of timely intelligence to policymakers and military leaders and that a review of the NRO was necessary to ensure that it was performing its tasks in a high-quality and cost-effective manner.

C. S. 2507, FY 2001 INTELLIGENCE AUTHORIZATION ACT

On April 27, 2000, the Committee reported S. 2507, the Intelligence Authorization Bill for Fiscal Year 2001. The Senate passed the bill on October 2, 2000, with several amendments. The bill, as passed by the Senate:

Authorized the intelligence activities and programs for the Central Intelligence Agency (CIA), the Department of Defense (DOD), the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the Department of the Army, the Department of the Navy, the Department of the Air Force, the Department of State, the Department of the Treasury, the Department of Energy (DOE), the Federal Bureau of Investigation (FBI), the National Reconnaissance Office (NRO), and the National Imagery and Mapping Agency (NIMA).

Criminalized the knowing and willful disclosure of classified information by persons with authorized access to such information to persons not authorized to receive the information. This provision was intended to close a gap in current law, which criminalizes only leaks of "defense information" or other specified categories of intelligence information. The Departments of Justice and State, the CIA, and the Executive Office of the President all supported the provision as adopted by the Senate.

Required the Director of Central Intelligence, in consultation with the Secretary of Defense, to create an analytic capability for intelligence relating to prisoners of war and missing persons. The analytic capability would extend to activities with respect to prisoners of war and missing persons after December 31, 1990.

Required the Director of Central Intelligence, in the wake of high profile security breaches at the State Department, to certify State Department compliance with applicable standards regarding the handling, retention, or storage of Sensitive Compartmented Information (SCI) material.

Strengthened the CIA Inspector General's (IG) Congressional reporting requirements in cases of possible wrongdoing by senior CIA officials, in response to the CIA's failure to report in a timely fashion, security violations by the former Director of Central Intelligence, John Deutch.

Amended the Drug Kingpin Act of 1999 to provide U.S. citizens with civil due process rights in the event their assets are seized or affected pursuant to the Act.

Amended the Intelligence Authorization Act for Fiscal Year 1995 and the Foreign Intelligence Surveillance Act to require additional coordination within, and among, the U.S. federal agencies investigating and prosecuting espionage and other cases affecting national security. It clarified, in statute, certain obligations of the affected agencies, ensured accountability in decisionmaking by agency heads, and codified current law and

practice with respect to determinations of "probable cause" under the FISA statute.

Created a Public Declassification Board, on a pilot program basis, that would be charged with advising the President on government-wide declassification efforts, while ensuring the protection of national security interests.

Created a process for the declassification of documents related to the Japanese Imperial Government similar to the process established for the Nazi War Crimes Disclosure Act.

S. 2507, as passed by the Senate, was supported by the Administration in a Statement of Administration Policy (SAP) issued on October 2, 2000. The Senate then requested a conference with the House and amended H.R. 4392 with the text of S. 2507, as amended.

In conference, all of the Senate provisions were included in the conference report except for the provision relating to the Drug Kingpin Act. House conferees argued that the Congress should not act with regard to this issue until the Judicial Review Commission on Foreign Asset Control issued its report as required by law. (The Commission issued a report on December 4, 2000 and the Committee expects to revisit the issue in the Fiscal Year 2002 authorization bill.)

The conferees also discussed section 304, relating to unauthorized disclosure of classified information, and section 501, relating to contracting authority for the National Reconnaissance Office. Amendments relating to both of these provisions were rejected by the conferees.

The conference report was approved, unanimously, by the Senate and the House on October 12, 2000. Unfortunately, despite the support of the heads of the affected agencies for section 304 and the previous written statements by the White House in support of the legislation, President Clinton vetoed the bill on November 4, 2000, citing his opposition to that provision.

Following the veto, on November 13, 2000, the House reintroduced and passed the conference report in the House as a new bill, H.R. 5630. H.R. 5630 did not include the provision regarding "leaks" of classified information that led to the President's veto. The Senate considered and passed H.R. 5630 on December 6, 2000, with an amendment by Senator Allard to strike section 501, relating to contracting authority by the National Reconnaissance Office. The House considered and passed the bill on December 11, 2000, without amendment. The President signed the bill on December 27, 2000 as P.L. 106–567.

D. S. 2089, THE COUNTERINTELLIGENCE REFORM ACT OF 2000

In response to some of the issues identified in the investigation of espionage at the Department of Energy labs, on February 24, 2000, Senators Specter, Torricelli, Thurmond, Biden, Grassley, Feingold, Helms, Schumer, Sessions, and Leahy introduced the "Counterintelligence Reform Act of 2000" (S. 2089). In early April 2000, the Select Committee on Intelligence held a closed hearing to receive testimony on S. 2089 and other issues involving the Foreign Intelligence Surveillance Act (FISA). The bill was considered by the Senate judiciary Committee on May 18, 2000, and ordered favorably reported with an amendment in the nature of a substitute. On

May 23, 2000, S. 2089 was reported to the Senate and immediately referred to the Select Committee on Intelligence pursuant to Senate Resolution 400, 94th Congress, on the same day. The Committee, by a vote of 15–0, ordered the bill favorably reported with amendments on July 18, 2000. The bill was considered by the Senate as an amendment by Senator Specter to the Intelligence Authorization Act for Fiscal Year 2001, and was enacted as part of that legislation (P.L. 106–567).

The bill delineates coordination responsibilities within and among the U.S. Government agencies investigating and prosecuting espionage cases and other cases affecting national security. The legislation clarifies, in statute, the obligations of each of the affected agencies in an espionage investigation, ensures accountability in decisionmaking by relevant agency heads, and codifies current law and practice with respect to a determination of "probable cause" under the FISA. The Committee's amendments to the bill are detailed in Senate Report 106–352, which accompanied S. 2089.

E. S. 1902, JAPANESE IMPERIAL GOVERNMENT DISCLOSURE ACT OF 2000

S. 1902, the Japanese Imperial Army Disclosure Act, was introduced by Senators Feinstein, Wellstone, Grams, Boxer, Levin, and Hatch on November 10, 1999. The bill was approved by the Judiciary Committee on May 18, 2000, without amendment, and referred to the Select Committee on Intelligence, pursuant to Senate Resolution 400, 94th Congress, on June 7, 2000. The Committee considered the legislation on July 18, 2000, and approved it with amendments.

The Act established a Japanese Imperial Army Records Interagency Working Group to review, for declassification, records pertaining to the Japanese Imperial Army and governments allied with, or cooperating with, the Imperial Army of Japan. The bill set out standards for the interagency working group to use, when reviewing the documents. In addition, it allowed for expedited processing of the Freedom of Information Act (FOIA) requests relating to Japanese Imperial Army records. The Committee amended the legislation to ensure the protection of intelligence sources and methods, by deleting a provision that would have eliminated the Director of Central Intelligence's obligation under the National Security Act of 1947 to protect operational files.

This legislation was considered by the Senate as an amendment by Senator Feinstein to S. 2507, the Fiscal Year 2001 Intelligence Authorization bill. That amendment was approved by the Senate, and the Japanese Imperial Army Records Disclosure Act was considered in conference as a Title of H.R. 4392. In conference, the provision was amended to apply to the Japanese Imperial Government rather than the Japanese Imperial Army and additional changes were made to ensure protection of sources and methods. The legislation was enacted as part of the authorization legislation (P.L. 106–567).

III. Oversight Activities

A. HEARINGS

1. Counterintelligence

In recent years, 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 trade craft in the 21st Century. The Committee made its views known to the nation's senior intelligence and counterintelligence officials. Many of them shared these concerns.

On March 8, 2000, during a closed hearing before the SSCI, DCI George Tenet, FBI Director Louis Freeh, and Deputy Secretary of Defense John Hamre unveiled a draft proposal entitled "Counterintelligence for the 21st Century." This plan, generally referred to as "CI 21," resulted from an extensive review assessing existing counterintelligence structures and capabilities to address emerging, as well as traditional, counterintelligence threats. The drafters of the CI 21 plan found current U.S. counterintelligence capabilities to be "piecemeal and parochial," and recommended adoption of a new counterintelligence philosophy—described as more policy-driven, prioritized, and flexible, with a strategic, national-level focus—as well as a restructured national counterintelligence system. CI 21 proposes significant changes in the way the United States Government approaches, and organizes itself, to meet the threat of foreign espionage and intelligence gathering.

After additional interagency review, the revised outlines of the CI 21 plan were presented to the Committee on July 26, 2000. The Committee will hold hearings on a Presidential Decision Directive (PDD) signed on December 28, 2000 establishing the CI 21 structures, authorities, and responsibilities.

2. Counterterrorism

Terrorism threatens American lives and interests around the world. The continuing and evolving terrorist threat was demonstrated by the October 12, 2000 terrorist attack on the USS *Cole* as it refueled in Aden, Yemen.[1] Ensuring that the Intelligence Community is well positioned to support the United States Government's efforts to counter terrorism remains among the Committee's highest priorities. In addition to extensive classified briefings at the staff level, the Committee held several hearings on the counterterrorism topic, as well as exploring counterterrorism issues in other hearings on the intelligence budget and other matters.

On February 9, 2000, the Committee held a hearing to receive the Intelligence Community's comprehensive assessment of the terrorist threat against the United States, the status of U.S. counterterrorism efforts, including the recent efforts to defeat the so-called "Millennium" threat, the resources devoted to countering the threat and any projected resource shortfalls.

The Committee subsequently received an off-the-record briefing by the Special Assistant to the President for National Security Af-

[1] The Committee's staff inquiry into the question of whether our intelligence capabilities were fully utilized prior to the attack on the USS *Cole* is addressed in this report's section on "Investigations and Inquiries."

fairs and National Coordinator for Counterterrorism, as well as the Director of the DCI's Counterterrorism Center, the FBI's Assistant Director for Counterterrorism and the Department of State's Coordinator for Counterterrorism.

On June 8, 2000, the Committee held an open hearing to receive the report of the National Commission on Terrorism, known as the "Bremer Commission," prepared pursuant to P.L. 277. Testifying before the Committee were Ambassador L. Paul Bremer III, Commission Chairman, as well as Commission Vice Chairman Maurice Sonnenberg, and Commissioners R. James Woolsey, Jane Harman, and Juliette N. Kayyem.

The purpose of the hearing was to inform the Committee of the intelligence-related findings and recommendations contained in the Commission's unclassified report entitled "Countering the Changing Threat of International Terrorism." The Committee noted that the Commission echoed the Committee's concern regarding the evolving threat posed by international terrorism. These concerns were noted in the Committee's May 4th report accompanying the Committee's Intelligence Authorization Bill for Fiscal Year 2001. In that Report, the Committee stated that: "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 Commission highlighted the Members' concern 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 Committee also noted, in that report, that the terrorist threats faced during the millennium celebrations were deferred rather than defeated.

In his opening statement, the Chairman applauded the Commission for highlighting the terrorist threat, the critical importance of intelligence in countering terrorism, and the need to fund and strengthen these capabilities, in particular human intelligence, on an urgent basis. The Commission also highlighted an urgent need to rebuild the National Security Agency. The Commission's report states that: "The National Security Agency is America's most important asset for technical collection of terrorism information, yet it is losing its capability to target and exploit the modern communications systems used by terrorists, seriously weakening the NSA's ability to warn of possible attacks." In this regard, the Commission Report cited the Senate Select Committee on Intelligence's Technical Advisory Group, whose reports on the NSA identify significant and expanding technology gaps. Rebuilding the NSA was the Committee's highest priority in its budgetary actions for Fiscal Years 2000 and 2001.

The Bremer Commission further raised concerns regarding policy restrictions that have impeded collection of intelligence by elements of the Intelligence Community legally authorized to undertake such collection. The Committee is continuing to review this issue as part of its on-going oversight.

3. Counterproliferation

There is no more disturbing trend than the proliferation of nuclear, biological, and chemical (NBC) weapons and the missiles to deliver them. As Director Tenet testified before the Committee,

"Over the next 15 years, . . . our cities will face ballistic missile threats from a wider variety of actors—North Korea, probably Iran, and possibly Iraq. * * * As alarming as the long range missile threat is, it should not overshadow the immediacy and seriousness of the threat that U.S. forces, interests, and allies already face overseas from short and medium-range missiles." At a minimum, American leaders seeking to defend U.S. interests overseas, against states or groups armed with such weapons, will have to reckon with an expanded threat of attack against U.S. forces, allies, or the U.S. homeland, dramatically changing their risk-benefit calculus in a given contingency.

On June 10, 1999, the Committee held a closed hearing to provide Members with an up-to-date understanding of the current proliferation threat and to assess the relative value of responses to counter or mitigate that threat. The Committee heard testimony from senior members of the Intelligence Community with responsibility for intelligence activities and analysis regarding proliferation, as well as from outside experts on proliferation issues.

The Committee also has received numerous briefings on proliferation-related topics, including a briefing on the export of military technology by the People's Republic of China (PRC). At the time, the Senate was about to consider two pieces of legislation relating to the PRC. The first was legislation proposed by Senator Thompson (S. 2645) that would require annual reviews of PRC proliferation activities and possible sanction of Chinese proliferators or other PRC activities. The second was legislation to grant the PRC permanent normal trade relations (PNTR) status (S. 2277)—a condition for final agreement between the United States and China to open the way for PRC membership in the World Trade Organization. Among the issues discussed in the Senate debate on these two bills were: Chinese proliferation; Chinese military and especially missile modernization, human rights abuses, the Chinese economy, and the impact of increased trade with the United States on democratization of the PRC. The purpose of the briefings was to provide Members with the current intelligence information regarding these issues in anticipation of Senate debate on the two bills.

4. Counternarcotics

The Committee held a closed hearing on July 29, 1999, to receive a general overview of the national security threat posed by international drug trafficking, as well as a description of the U.S. Government's efforts directed against this threat. The situation in Colombia was addressed in detail, with particular emphasis placed on those Colombian insurgent groups which actively participate in, and derive their funding from drug trafficking.

While the primary focus of the hearing was on Colombia, the witnesses also presented information on those foreign governments, or defacto governments, that actively participate in, or provide support for drug trafficking. This discussion included information regarding the Revolutionary Armed Forces of Colombia (FARC), the insurgent group which controls nearly two-thirds of Colombian territory, and the Taliban regime in Afghanistan. Additionally, the witnesses discussed the merits of establishing a component within the Drug Enforcement Administration to facilitate the sharing of

intelligence valuable for national security while protecting law enforcement and prosecutorial equities.

5. Denial and deception

The Committee has been deeply concerned about the increase in foreign denial and deception efforts directed against U.S. intelligence collection. Denial and deception refers to efforts to conceal, or mislead with respect to, activities of interest and concern to U.S. policymakers such as military deployments, development of weapons of mass destruction, and political intentions. Denial and deception threatens the national security by depriving U.S. policymakers and military leaders of timely and accurate intelligence of threats to U.S. interests. The Committee held one briefing for Members and a number of staff briefings on denial and deception issues. The Committee increased funding for activities to counter denial and deception, and has directed actions designed to focus Intelligence Community resources and management attention on this critical intelligence challenge.

6. Ballistic missile analysis

As discussed elsewhere in this report, a critical threat facing the United States today is the threat of attack by ballistic missiles bearing nuclear, biological or chemical weapons. The Intelligence Community has no more serious challenge than to monitor this threat and no more serious responsibility than to get this analysis right. On September 30, 1999, the Committee held a closed hearing to receive testimony from the National Intelligence Officer for Strategic and Nuclear Programs on the analysis and findings of a National Intelligence Estimate (NIE) titled "Foreign Missile Developments and the Ballistic Missile Threat to the United States Through 2015." The NIE concluded that during the next 15 years the United States most likely will face Intercontinental Ballistic Missile (ICBM) threats from Russia, China, and North Korea, probably from Iran, and possibly from Iraq, although the threats will consist of dramatically fewer weapons than today due to significant reductions expected in Russian strategic forces.

The Committee found that the NIE incorporated a number of improvements in the rigor and quality of the analysis, including many based on the recommendations of the Commission to Assess the Ballistic Missile Threat to the United States (also known as the Rumsfeld Commission) in its July 1998 Report.

7. State Department security breaches

During the 106th Congress, the Committee held hearings and staff briefings to review significant security breaches that occurred at the Department of State. The Committee believes this series of incidents reveals serious deficiencies in security awareness, practice, and culture at the State Department.

In February 1998, an unidentified man, wearing a tweed jacket entered the Secretary of State's seventh floor office suite and removed classified documents, including documents classified as Sensitive Compartmented Information (SCI). The man, in this "tweed jacket incident" has never been identified and the documents have never been recovered. Additionally, poor procedures for handling classified information resulted in the Department's inability to re-

construct which documents were taken. Without such information, a full and complete damage assessment was not possible.

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's detention 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. Gusev was declared persona non grata and was required to leave the United States.

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.

In January 2000, a laptop computer containing highly sensitive classified intelligence materials, including SCI material relating to weapons proliferation, was discovered to be missing from the State Department Bureau of Intelligence and Research (INR) and is presumed stolen. Despite an obligation under the National Security Act of 1947 to keep the intelligence committees "fully and currently informed of all intelligence activities" including "significant intelligence failures," the Committee was not informed of the loss of this laptop computer until after the Washington Post reported the story in April 2000.

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 September 1999 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) In response to the IG Report in the Annex to the Intelligence Authorization Act for Fiscal Year 2000, the Congressional intelligence committees required (1) a report from the DCI evaluating the State Department's compliance with all DCIDs related to the protection of Sensitive Compartmented Information, (2) a State Department report on specific plans for enhancing the security of classified information within the State Department and (3) full implementation, as appropriate, of the recommendations found within the Inspector General's report.

The February 2000 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 docu-

ment control and accountability." In its report the State Department identified a number of actions or proposed actions it intended to take in response to the IG Report.

In the wake of the missing laptop computer incident, Secretary of State Albright declared her intention to transfer positions and responsibility for ensuring the proper security and handling of SCI material from the State Department's Bureau of Intelligence and Research to the Bureau of Diplomatic Security (DS). At that time, the Committee expressed its concerns regarding this transfer, including the need to ensure continued DCI oversight over SCI material at the State Department and the requirement that this function should be funded through the National Foreign Intelligence Program (NFIP) budget. Such oversight and budgetary authority is critical to ensure effective implementation of measures to protect intelligence information at the State Department. In the fall of 2000, the DCI's Community Management Staff and the Department of State agreed to measures designed to ensure continued DCI oversight of the protection of SCI material and continued funding for this function within the NFIP.

In the Intelligence Authorization Act for Fiscal Year 2001, the Committee required the Director of Central Intelligence, in the wake of high profile security breaches at the State Department, to certify State Department compliance with applicable standards regarding the handling, retention, or storage of Sensitive Compartmented Information material. Elements of the State Department that the DCI does not certify as in compliance, or that do not receive a DCI waiver, may not retain or store SCI information until they are certified as compliant.

Additionally, the Committee, in the report accompanying the Intelligence Authorization Act for Fiscal Year 2001, directed the State Department Inspector General to conduct annual reviews of State Department policies and procedures for protecting classified information at the State Department for the next five years to determine progress in this area.

The Committee has taken numerous steps to improve the security situation at the State Department and will continue this focused oversight in the future.

8. National security threats to the United States

The Committee continued its practice of opening each new session of the Congress with open and closed hearings reviewing the Intelligence Community's assessment of current and projected threats to the national security of the United States. These annual hearings form the backdrop for the Committee's budget authorization process, as well as provide a rare public forum for discussion of national security threats by the nation's top intelligence officials.

In his February 2, 2000 appearance before the Committee, Director of Central Intelligence George Tenet emphasized the interplay between traditional and emerging threats and modern military technologies, in particular, ballistic missiles, chemical, nuclear and biological weapons, and information technologies.

"Over the next 15 years * * * our cities will face ballistic missile threats from a wider variety of actors [in addition to Russia and the PRC]—North Korea, probably Iran, and possibly Iraq," the DCI testified. The DCI noted that, "in a very real sense, we live at a

moment when the past and the future are colliding. In other words, today we must still deal with terrorists, insurgents, and others who have hundreds of years of history fueling their cases—but the chances are they will be using laptop computers, sophisticated encryption, and weaponry their predecessors could not even have imagined."

The DCI expanded upon these themes, noting that traditional ethnic hatreds and conflicts once frozen within the global competition between two Cold War superpowers are now thawing in Africa, the Caucasus, and the Balkans. At the same time, a growing perception of so-called American "hegemony" has become a lightening rod for the disaffected. Such an environment of rapid change makes the United States even more vulnerable to sudden surprise.

Throughout the 106th Congress, the Committee focused on these and other threats and challenges to the security of the United States. It concentrated much of its attention on unconventional and asymmetric threats, including threats posed by the proliferation of weapons of mass destruction and high-technology, and state-sponsored and non-state terrorism. In particular, the Committee recognizes that this dynamic change and uncertainty continues, driven by significant transitions in key states and regions throughout the world, the activities of "rogue" states and terrorist groups, rapid technological development and proliferation, continuing international criminal activity, and resentment of U.S. political, economic, military, and social dominance.

The transcript of the Committee's February 2, 2000 hearing, "Current and Projected National Security Threats to the United States" (S. Hrg. 106–580) was printed and made available to the public.

9. Covert action quarterly review

Throughout the 106th Congress, the Committee continued to conduct rigorous oversight of covert action programs. The Committee reviews these programs to ensure their methods and objectives are consistent with U.S. foreign policy goals, and are conducted in accordance with all applicable U.S. laws. The Committee pursues its oversight responsibilities with the understanding that covert action programs can be a significant factor in accomplishing vital foreign policy objectives. At the same time, to be successful, such programs must be consistent with the ideals and principles of our nation. During the 106th Congress, the Committee established, with the Central Intelligence Agency and the National Security Council, a process to conduct regular quarterly written assessments of the covert action programs. The Committee believes this reporting requirement will improve both the implementation and oversight of covert action programs in the future.

10. Kosovo

In the 106th Congress, the Committee closely monitored developments in Serbia and Kosovo and the corresponding intelligence issues that emerged in the course of NATO's first-ever offensive combat operations. The Committee has continued to follow events in the former Yugoslavia, including intelligence issues relating to the NATO implementation force in Kosovo, and analysis of recent political developments in Serbia.

The Committee examined the intelligence track record with regard to the crisis in Kosovo and the Balkans—what we knew, when did we know it, what were the analysts telling the policymakers?

On April 14, 1999, the Committee held a closed briefing on the military and intelligence implications of the crisis in Kosovo, with testimony by General John Gordon, Deputy Director of Central Intelligence; General Patrick Hughes, Director of the Defense Intelligence Agency; and Phyllis Oakley, Assistant Secretary of State for Intelligence and Research.

The Committee also was interested in how the worldwide U.S. collection posture was affected by the Balkan crisis, with special emphasis on hard target coverage. Finally, the Committee undertook an examination of collection requirements and opportunities facing the United States and the NATO Alliance in Kosovo.

In 2000, the Committee focused on the "intelligence lessons learned" from the Kosovo military campaign, culminating in a May 10, 2000 briefing from the outgoing Supreme Allied Commander Europe, General Wesley Clark. That briefing touched on the problems associated with NATO Alliance intelligence sharing during the air campaign and the implications for timely intelligence of the "war-making-by-committee" approach that characterized the early stages of the Kosovo operation.

11. Russia

Over the past two years, the Committee has sought to stay abreast of fast-paced developments in Russia by holding closed briefings on the full range of national security and intelligence issues associated with these changes. The Committee has concentrated its attention on issues associated with Russia's proliferation of nuclear and missile technology, especially to Iran, Russia's evolving security relationship with the PRC, as well as monitoring Russian nuclear issues.

Russia's interests coincide with those of the United States and our allies from time to time. They often do not. Regional instability in the former Soviet Union, in particular in the Caucasus or Central Asia, could threaten U.S. interests, especially if such instability were to spiral out of control or tempt external intervention.

The long term impact of the Duma elections in December 1999, Yeltsin's surprise resignation, and the advent of Vladimir Putin as Yeltsin's successor remain unclear. The Committee focused its attention on how these recent leadership changes will affect Russian's foreign and security policies. Although Russia's need for integration into international economic institutions and access to financing and key markets may make a wholesale return to the confrontation of the Cold War unlikely, Russia, especially under Putin, is likely to persist in efforts to counter what it perceives as U.S. dominance by using all the tools remaining at its disposal.

Russian domestic developments will have a great inpact on stability in Eurasia and on Russia's capacity to act abroad. The Committee recognizes that the United States has a major interest in Russia's domestic transformation, although our ability to affect the outcome is severely limited.

12. The People's Republic of China (PRC)

The People's Republic of China is perhaps the preeminent national security, foreign policy, and intelligence challenge facing the United States in the post-Cold War world. In the 106th Congress, the Committee held a total of 26 hearings on a wide range of intelligence, counterintelligence, and policy issues relating to the PRC. Many of these activities are described in greater detail in sections of this report covering the Committee's investigations into missile and satellite technology transfers to the PRC and PRC efforts to influence U.S. policy, and PRC nuclear espionage, Department of Energy counterintelligence and security matters, and the Wen Ho Lee investigation and prosecution.

Given the PRC's emergence as a strategic competitor of the United States, it is critical that U.S. policymakers have a complete, objective, and accurate understanding of the goals, intentions, motivations, capabilities, and prospects for change of the world's most populous nation. To that end, the Committee directed actions to ensure that the CIA Directorate of Intelligence applies rigorous external contrarian scrutiny to its analysis of the PRC.

13. Colombia

On January 25, 2000, President Clinton announced a Colombia Assistance Package to help "strengthen the Colombian economy and democracy, and fight narcotics trafficking." The assistance package totals approximately $1.3 billion spread over fiscal years 2000 and 2001. The assistance provided by the United States is part of a $7.5 billion plan set forth by Colombian President Andres Pastrana to battle Colombia's narcotics, military, and economic problems. Colombia plans to provide $4 billion towards this effort with the remainder coming from other international assistance. "Plan Colombia" has five major components: helping the Colombian Government push into the coca-growing regions of southern Colombia, which are now controlled by insurgent guerrillas; upgrading Colombian capability to aggressively interdict cocaine and cocaine traffickers; increasing coca crop eradication; promoting alternative crops and jobs; and increasing protection of human rights, expanding the rule of law, and promoting the peace process.

On February 3, 2000, the Committee held a closed hearing on the situation in Colombia, with specific focus on the proposed assistance package and additional funding for intelligence activities included in the President's supplemental appropriations request The witnesses were asked to provide analysis on the political and military situations in Colombia; to describe current narcotics trafficking activity within that nation; to explain the rationale for the $1.3 billion supplemental request for Colombia; and to describe how additional intelligence funding would be used. The hearing also explored the involvement of armed guerrilla groups and paramilitaries in the drug trafficking business. The Committee will continue to monitor closely developments in Colombia and the contribution of U.S. intelligence agencies to U.S. policy.

14. Iraq

During the 106th Congress, the Committee continued its extensive oversight of intelligence collection and analysis in support of U.S. policy towards Iraq. Since the end of the Gulf War, Iraq's in-

transigent rejection of United Nations resolutions regarding Iraq's programs to develop weapons of mass destruction, unwillingness to accept international inspectors, and continued belligerence towards its neighbors have been a serious concern for the United States and its allies. Throughout this period, American military personnel have been in a constant state of alert and are often engaged in combat operations in the course of enforcing the northern and southern no-fly zones established in Iraq in the wake of the Gulf War.

In 1999 and 2000, the Committee held a number of closed hearings and briefings to review intelligence collection and analysis on Iraq, intelligence support to U.S. military forces in the area, and support to the efforts initiated under the Iraqi Liberation Act (ILA) of 1998. In addition, Committee members and staff received numerous classified briefings throughout the 106th Congress on intelligence regarding Iraq's missile, chemical, biological, and nuclear programs, and the status and intentions of Saddam Hussein's regime.

15. India/Pakistan

In the summer of 1999, after five decades of tension and three wars, Pakistan and India engaged in military clashes over Kashmir. Fighting between India and Pakistan and India and Kashmiri separatists resulted in more than a thousand casualties. Tensions remained high in 2000. The acquisition of nuclear weapons capability by both countries, demonstrated by nuclear tests in 1998, heightens concern that tensions between India and Pakistan could erupt with little warning into full-scale war, possibly escalating rapidly to nuclear war. Providing warning in such a situation is a critical challenge for the U.S. Intelligence Community.

In addition to staff briefings, on May 24, 2000, the Committee received a classified briefing by senior intelligence officers on India and Pakistan. The purpose of this briefing was to provide Members with an update on the ongoing tensions between India and Pakistan and the current status of their military capabilities.

16. Cyber security

The United States increasingly has become reliant on certain critical infrastructures, i.e., the physical and computer-based systems essential to the operation of the economy, government, and public health and safety. These include telecommunications, energy, banking and finance, transportation, water systems, and both governmental and private emergency services. On July 22, 1999, the Committee held a closed hearing to review the Intelligence Community's role in securing our nation's critical information infrastructure.

As the information technology revolution links and automates critical components of our infrastructure, our reliance on computers and advanced telecommunications creates a new potential vulnerability to computer attack, in addition to the more traditional threats from physical attack, equipment failure, human error, and weather.

During the 106th Congress, Committee Members and staff had numerous classified briefings regarding the role of the Intelligence Community in identifying information warfare threats and warn-

ings, and in providing technical expertise to both defend against computer attacks and investigate actual computer intrusions. The Committee will continue its oversight of this growing threat to our national security.

17. Y2K

On September 15, 1999, the Committee held a closed hearing on the Year 2000 (Y2K) computer issue and its potential impact on the U.S. and other nations.

The Y2K problem originated from the lack of information storage capacity in the first few generations of computers. Because storage capacity was at a premium, programmers decided to designate a year by its last two digits (i.e., 88 instead of 1988) in order to save computer memory space. This practice was common until the mid–1990s. As a result many computer experts feared that older computer hardware devices and software would incorrectly recognize the two digits representing the year 2000 (00) as the year 1900, and that this problem would cause computer hardware and software to freeze up or shut down. Also, because computers connected in a network are interdependent, newer systems connected to hardware and software susceptible to the Y2K problems also would suffer difficulties even if the newer systems were Y2K compliant. Many believed that the Y2K problem had the potential to cascade through computer networks or systems dependent on computers susceptible to the Y2K problem.

While the U.S. Government and American companies applied significant time and resources to addressing the Y2K issue prior to December 1999, information technology experts expressed concern that most foreign governments and companies had not adequately prepared for this problem. As a result many computer experts feared that Y2K failures might cause catastrophic failures in these nations' industrial sectors and facilities.

The Intelligence Community prepared analyses on the possible effects of the Y2K problem in various nations, and how these consequences could have affected U.S. policy and interests abroad. Despite alarmist predictions by both the Intelligence Community and private sector analysts, the vast majority of computer systems worldwide were prepared for the Y2K issue and the failures that did occur were adequately contained and remedied without significant damage.

18. Lt. Commander Michael Speicher

U.S. Navy Lt. Commander "Scott" Speicher was shot down over Iraq on January 17, 1991, the first night of the Gulf War. He was subsequently declared "Killed in Action" (KIA). For several years, the Committee has been concerned that LCDR Speicher has never been adequately accounted for.

The issue surfaced in the 105th Congress when the New York Times ran a front page article that reported that Admiral Stanley Arthur, then Vice Chief of Naval Operations and formerly Commander of Allied Naval forces in the Persian Gulf during the Gulf War, believed "that Commander Speicher had ejected successfully and survived." The Committee's interest centered on the role and impact of intelligence on the Government's accounting of LCDR Speicher, and what the Committee increasingly came to view as

the discrepancy between the available intelligence information and the Navy's determination that LCDR Speicher had been killed on the night of January 17, 1991.

In July 1999, Senator Pat Roberts asked the SSCI to conduct an inquiry into the Intelligence Community's input to the U.S. Government's decision to list LCDR Speicher's status as KIA.

The Committee held a closed briefing on September 15, 1999, and a closed hearing on October 28, 1999, to examine the case. The Committee received testimony from Vice Admiral Thomas Wilson, Director of the DIA, Brigadier General Roderick Isler, Associate DCI for Military Support and Admiral Mike Ratliff, Director of Naval Intelligence. The purpose of the hearing was to: (1) review the Intelligence Community's analytical input concerning Speicher's status as a Prisoner of War, Missing, or Killed in Action, (2) determine how the Intelligence Community is organized to carry out the DCI's statutory responsibility for analytical support on POW/MIA matters and, (3) consider recommendations for handling analysis of POW matters in the future. The Committee concluded that information existed suggesting that LCDR Speicher may have survived his aircraft being shot down. If so, he may at one time have been—and conceivably could still be—a prisoner of war.

The Committee's interest prompted the establishment of a Secretary of Defense "Tiger Team," which included members of the DIA and the Office of the Secretary of Defense (OSD), to reassess the Speicher case. Although scheduled to produce a joint report on March 13, 2000, DIA and OSD were unable to agree on findings, and no report was published. The Committee held an additional closed hearing on April 4, 2000. The Committee received testimony from Vice Admiral Wilson; Jerry M. Hultin, Under Secretary of the Navy; and Mr. Paul Lowell, Director of Naval Intelligence. The purpose of the hearing was to (1) review the Intelligence Community's all-source analytical input to the Secretary of the Navy and the DoD Tiger Team concerning Speicher's status, (2) review the Intelligence Community's responsiveness to the Secretary of the Navy's intelligence needs regarding the Speicher case, and (3) determine how the Intelligence Community might be better organized to carry out the DCI's statutory responsibility for analytical support on POW/MIA matters.

At this hearing, Members learned that no comprehensive analytic review of all-source intelligence had been produced on the fate of LCDR Speicher since his plane was shot down in 1991. As a result, the Committee directed a comprehensive analytical assessment of the intelligence related to the fate of LCDR Speicher. The Committee held another closed briefing on July 25, 2000, to update Members on efforts to obtain the fullest possible accounting of LCDR Speicher's fate. The Committee, by that point was deeply concerned that the Navy's conclusion that LCDR Speicher was killed in action during the Gulf War did not reflect the information provided by the Intelligence Community. In addition, the Committee directed that the Inspectors General of the Department of Defense and the Central Intelligence Agency jointly examine the intelligence support to the Speicher case and address (1) the Intelligence Community's organization and assignment of responsibility,

(2) dissemination of reporting, and (3) objectivity, accuracy, and completeness in handling POW/MIA issues.

Largely as the result of the collection and analytic efforts directed by the Committee, the Navy on January 10, 2001 changed LCDR Speicher's status from "Killed in Action" to "Missing in Action." On the same day, the State Department delivered a demarche and diplomatic note to the Iraqi Interests Section in Washington demanding an accounting of any information regarding Commander Speicher's fate.

19. Nazi War Crimes

The Committee met on September 16, 1999 to review the status of declassification efforts by the Intelligence Community to comply with the Nazi War Crimes Disclosure Act of 1998. The purpose of the law is to ensure that information contained in classified World War II documents will be made available to the public through declassification. Senators Shelby, DeWine, Hatch, and Kyl co-sponsored this Act.

The Committee heard from members of the Intelligence Community, the Chairman of the Nazi War Criminal Records Interagency Working Group, and officials from the Office of the Secretary of Defense.

The testimony indicated that declassification efforts are proceeding well; records are being stored in the National Archives; and there are no fiscal or organizational impediments to sustaining this effort. The Working Group was given a two year extension as part of the Japanese Imperial Government War Crimes Act.

20. Encryption

The Committee is concerned by the impact of widespread encryption on the NSA's ability to collect signals intelligence on threats to U.S. interests, and on the ability of the FBI and other law enforcement agencies to conduct their counterterrorist, counterintelligence, and law enforcement missions. Encryption is the process of disguising a message in such a way as to hide its content. Historically, encryption has been used primarily by governments and militaries to protect their diplomatic communities, military plans, and other secrets. However, in the last two decades the growing use of computers, computer networks, the Internet cellular telephones and other telecommunications technologies has increased the demand for encryption products to protect privacy and confidentiality.

Modern encryption products use complex mathematical algorithms to encode messages. The strength of an encryption product normally is judged according to the number of "bits" in the key—the higher the number of bits, the stronger the encryption. Until recently, the export of encryption products had been tightly regulated due to concerns over how the availability and use of strong encryption products overseas would affect the NSA's capability to collect signals intelligence (SIGINT).

During the 106th Congress, the Committee reviewed numerous bills and proposals regarding encryption policy, and received classified briefings regarding how the Intelligence Community seeks to adjust to the use of modern encryption products.

On September 22, 1999, the Committee held a closed hearing to hear the recommendations contained in the Committee's TAG review of U.S. encryption policy. The TAG members were asked to address (1) the seriousness of the technical challenge to foreign intelligence collection posed by commercial encryption products, (2) alternative technical responses to the proliferation of encryption products, (3) the viability of the foreign encryption products market, (4) federal policy or statutory prescriptions that will protect national security interests, and (5) technical or policy alternatives that will assist law enforcement to gain access to encrypted information in accordance with legal and constitutional safeguards.

The Committee will maintain its oversight of U.S. encryption policy and will continue to support the Intelligence Community's plans to address encryption technology.

21. Comprehensive Test Ban Treaty (CTBT)

In October 1999, the Committee held a closed hearing with senior representatives of the Intelligence Community in support of the Senate's deliberations on whether to give its consent to ratification of the Comprehensive Test Ban Treaty. The hearing focused on the ability of the United States to monitor foreign nuclear testing in the context of the treaty and the relative contributions of national and international monitoring and inspection capabilities. Later in the month, the Senate voted against U.S. ratification of the Comprehensive Nuclear Test Ban Treaty.

The Committee also held staff briefings on possible Russian nuclear test activities and the other aspects of foreign nuclear weapons programs affecting U.S. national security.

22. The Foreign Intelligence Surveillance Act (FISA) and the technology challenge

In 1998, the Committee audit staff conducted a six-month, comprehensive review of the implementation and administration of the Foreign Intelligence Surveillance Act of 1978. While the audit staff found that the FISA legal review and approval procedures receive senior management attention and are appropriately rigorous, effective, and consistent with the law, the staff also found that certain agencies were not prepared to counter emerging technologies which challenge traditional techniques of intelligence gathering under the FISA.

The challenges the Intelligence Community faces in conducting electronic surveillance in today's communications environment remain a particular concern to the Committee. As the FISA has been the means by which some of our nation's most important intelligence has been obtained for more than two decades, it is imperative for the intelligence oversight committees to understand the impact the dramatic changes in communication and information technology have had on FISA collection efforts. Equally important is the need to ensure that the FISA statute itself keeps pace with rapidly changing technology, so that counterintelligence and terrorist targets cannot evade detection and prosecution by simply changing the way they communicate, and at the same time, to ensure that the privacy rights of American citizens are not placed at risk.

In March 2000, the Committee conducted a hearing to review the role and viability of the FISA in today's collection environment and the impact of modern technology. Senior Intelligence Community officials have told the Committee that the Act of 1978 presently provides the flexibility to permit collection against emerging technologies.

The Committee also is encouraged by recent Intelligence Community efforts both to confront technological changes and exploit opportunities presented by rapidly changing communications technologies. However, the Committee recognizes that any degradation in the Intelligence Community's capability to exploit emerging communications technologies will adversely affect our nation's ability to collect critical intelligence information. Monitoring of the Intelligence Community's research and development efforts to ensure that collection capabilities keep pace with communications technologies will continue to be a high priority for the Committee's oversight of the FISA.

23. Pan Am 103

On December 21, 1988, Pan Am Flight 103 exploded in the air over Lockerbie, Scotland. The explosion and crash killed 270 people, including 189 Americans, and was quickly determined to have been the work of terrorists. On May 3, 2000, more than 11 years after the bombing, the trial under Scottish law of two Libyan nationals, Abdel Basset Ali al-Megrahi and Lamen Khalifa Fhima, began in Camp Zeist, The Netherlands. [The Scottish Court convicted Fhima and acquitted al-Megrahi for the bombing in February 2001.]

This Committee monitored the proceedings in The Netherlands as part of its oversight responsibilities. The United States Government and, in particular, the Director of Central Intelligence pledged full support to the Scottish prosecutors in their efforts to obtain a conviction of the two Libyan nationals. The Committee supports that commitment. The families of the American citizens who died in that explosion have a right to expect that the United States Government will go to extraordinary lengths to bring the perpetrators to justice. Those who may plan to engage in terrorist acts against United States citizens or interests in the future must know that the United States will pursue justice no matter how long it takes.

In a briefing to the Committee on March 3, 2000 Members were briefed on the CIA's role in providing information in its possession to support the prosecution, which is unprecedented in a case heard before a foreign tribunal. In addition to the briefing for Members, the Committee staff received periodic briefings on the progress of the case, particularly with respect to the potential risks to intelligence sources and methods caused by the introduction of CIA documents as evidence and the testimony of CIA officers as witnesses.

24. Intelligence needs of Unified Commands

For the first time since the formation of the Senate Select Committee on Intelligence, the Committee conducted a briefing for Members with the senior intelligence officers of the Unified Combatant Commands and the Specified Commands. The Committee

held the briefing to assess the levels of support provided by the Intelligence Community to the commands.

The conclusion of the Cold War and the spread of technologies related to weapons of mass destruction have complicated the plans and intelligence requirements within the commands. Preventing strategic surprise remains an important mission, but terrorism, counternarcotics, peacekeeping and humanitarian support require increased emphasis to meet the diverse mission requirements of the commands.

By consensus, the commands have been satisfied with the level of support provided by the Intelligence Community. There is agreement, however, that the imbalance between collection and processing, exploitation and dissemination continues to grow. While strongly supporting new collection platforms, the commands would like to see greater emphasis placed on processing, exploitation, and dissemination capabilities.

25. National Imagery and Mapping Agency (NIMA) and tasking, processing, exploitation, and dissemination (TPED) modernization

The Committee long has 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 of intelligence collected by satellites, airplanes, unmanned aerial vehicles, and other platforms and sensors. The issue of Tasking, Processing, Exploitation, and Dissemination Modernization 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 NIMA issued a congressionally-mandated report describing the challenges and projected shortfalls in the areas of TPED related to 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 Committee concluded that Phase One of the Administration's three phase TPED modernization plan was 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 was 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 Committee was concerned that the dramatic underfunding of Phase One TPED modernization in fiscal year 2001 was setting up a budgetary crunch wherein a disproportionate amount of funds would be required in subsequent years of the FYDP.

The Committee held a closed hearing on March 2, 2000, to hear testimony on the objectives and plans of the NIMA to meet the needs of the national and military intelligence customers today and in the future. One area of particular concern to the Committee was

the modernization effort underway concerning imagery and geospatial TPED. Arthur Money, Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and Lieutenant General James King, Director of the NIMA, testified before the Committee on the Administration's plan to address the TPED shortfalls in Fiscal Year 2001 and over the balance of the FYDP time frame. Dr. Anita Jones testified on the findings contained in a just-completed report of the Defense Science Board Task Force, which she co-chaired, reviewing the NIMA's roles and missions and TPED modernization strategy.

The Committee recommended 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.

26. Unauthorized disclosure of classified information

On June 14, 2000, the Committee held a hearing to review recent significant instances of the public release of classified information, to determine how the release of classified information has affected intelligence collection, to discuss how these cases are investigated and prosecuted, and to consider ways to halt such "leaks" of classified information. The witnesses at this hearing included Attorney General Janet Reno, DCI George Tenet and FBI Director Louis Freeh.

Over the past five years, information regarding a number of sensitive intelligence collection programs and assets has appeared in the press. These leaks include information that endangers human intelligence sources, information about our nation's satellite collection systems, and various signals intelligence information on terrorist, proliferation, and other targets.

The public release of such material can result in the loss of access to intelligence, the enhancement of denial and deception techniques, an increased reluctance of current and potential assets to work for the United States, and the arrest, imprisonment, and execution of foreign human assets.

The Bremmer Commission Report, titled "Countering the Changing Threat of International Terrorism" stated that "[l]eaks of intelligence and law enforcement information reduce its value, endanger sources, alienate friendly nations and inhibit their cooperation, and jeopardize the U.S. Government's ability to obtain further information."

In most leaks cases, the identity of the person who released the classified information is unknown. In many instances, the classified information was widely distributed, with literally hundreds of people having access to the intelligence report. This limits the ability of law enforcement officials to identify a possible source.

Currently, there is no general criminal penalty for the unauthorized disclosure of classified information. There are statutes prohibiting the unauthorized disclosure of certain types of information, such as diplomatic codes, nuclear information, communications intelligence, or "national defense" information. Many leaks of classified information do not easily fit within existing statutory definitions, for example, certain intelligence information from human sources and some information relating to covert action. Some legal

scholars have argued that existing statutes only apply to classic espionage situations and are not meant to be applied to "leaks."

The Committee sought to address this issue in the fiscal year 2001 intelligence authorization bill. Section 304 of the Intelligence Authorization Act for Fiscal Year 2001 would prohibit any current or former officer, employee, or contractor with access to "classified information" from knowingly and willfully disclosing it to unauthorized personnel. "Classified information" was defined within this section as:

> "* * * information or material designated and clearly marked or represented, or that the person knows or has reason to believe has been determined by appropriate authorities, pursuant to the provisions of a statute or Executive Order, as requiring protection against unauthorized disclosure for reasons of national security."

After the Committee had received approval from and support for this provision from the Administration, President Clinton vetoed the Intelligence Authorization Act for Fiscal Year 2001 based upon the inclusion of this provision.

Following the veto, on November 13, 2000, the House reintroduced and passed the conference report in the House as a new bill, H.R. 5630. H.R. 5630 did not include the provision regarding "leaks" of classified information that led to the President's veto. The Senate considered and passed H.R. 5630 on December 6, 2000, with an amendment by Senator Allard to strike section 501, relating to contracting authority by the National Reconnaissance Office. The House considered and passed the bill on December 11, 2000 without amendment. The President signed the bill on December 27, 2000 as P.L. 106–567.

The Committee will continue its oversight of efforts to prevent and investigate unauthorized disclosures of classified information, and may seek to reintroduce legislation in the 107th Congress to address the insufficient statutory prohibitions against leaks of classified information.

B. INVESTIGATION AND INQUIRIES

1. The People's Republic of China investigations

In the 105th Congress, the Committee unanimously approved Terms of Reference for investigations into "Impacts to U.S. National Security of Advanced Satellite Technology Exports to the People's Republic of China (PRC)" and "The PRC's Efforts to Influence U.S. Policy."

These investigations were prompted by (1) press reports of possible export control law violations by Loral Space and Communications Ltd. and Hughes Electronics Corporation, in the course of launching U.S. satellites on Chinese rockets that may have harmed U.S. national security by providing expertise to the PRC's military ballistic missile programs, and (2) a report that Johnny Chung, a Democratic Party fund-raiser, being investigated for improprieties during the 1996 presidential campaign, told Department of Justice investigators that an executive with a PRC aerospace company gave him $300,000 to donate to President Clinton's 1996 re-election campaign. The latter report came against a backdrop of earlier re-

porting and prior congressional investigations of a PRC Government plan to influence the American political process.

Subsequent investigations and press reporting identified additional problems in the course of U.S. satellite launches in the PRC, which were first authorized under a policy dating to the Reagan Administration, designed to address the shortage of space launch capabilities following the Challenger disaster. These problems included Hughes' transfer to the PRC of a failure analysis of the 1995 launch of the Hughes Apstar 2 satellite, and the absence of U.S. Government monitors at Chinese launches of three Hughes satellites in 1995–1996. Other press reports raised concerns that the PRC may have developed technology applicable to Multiple Independently Retargetable Vehicles (MIRVs) through its development, to U.S. specifications, of a multiple-satellite "Smart Dispenser" to place Motorola "Iridium" communication satellites in orbit.

In the course of its investigations, which concluded in May 1999, the Committee conducted ten hearings and dozens of staff briefings and interviews. Witnesses included the Director of Central Intelligence George Tenet, Attorney General Janet Reno, FBI Director Louis Freeh, and expert witnesses from the CIA, the Defense Department's Defense Technology Security Administration (DTSA), the Department of State, the National Air Intelligence Center (NAIC), the NSA, the DIA, and the General Accounting Office (GAO). Committee staff also reviewed tens of thousands of documents provided by Executive departments and agencies and U.S. satellite manufacturers, and produced analyses for the Committee's use based on those documents.

In a Committee Report approved on May 5, 1999, by a vote of 16 to one, the Committee found, with respect to satellite and missile technology transfers, that:

> The technical information transferred during satellite launch campaigns enables the PRC to improve its present and future space launch vehicles and ICBMS. Because such analyses and methodologies are also applicable to the development of other missile systems, the Committee believes that, where practicable, the PRC will use the transferred information to improve its short range ballistic missiles (SRBMs), intermediate range ballistic missiles (IRBMs), and related technology. These missiles could threaten U.S. forces stationed in Japan and Korea, as well as allies in the region.
>
> * * * * *
>
> The Committee's conclusions with respect to technology transfer are based on the evidence of technology transfers to the PRC's space launch industry * * * the substantial similarities between space launch vehicles and ballistic missile technology (the CIA has described space launch vehicles as ballistic missiles in disguise), the integration of the PRC's space launch and ballistic missile industries, the PRC's intention to modernize and upgrade its ballistic missile force, evidence that U.S. know-how was incorporated into the PRC space launch program, and the Committee's assumption that any improvements in the PRC's space

launch vehicles would be incorporated wherever practicable in the PRC's military ballistic missile program.

* * * * * * *

In the past, the PRC has proliferated SRBMs, IPBMs, and their related technology to potential U.S. adversaries such as Iran and to countries such as Pakistan where the presence of advanced weapons increases regional instability. U.S. national security interests already may have been harmed if the PRC used the transferred information to improve these proliferated missile systems. Or U.S. national security may be harmed in the future if the PRC proliferates missile systems or components that have been improved as a result of the technology transfer.

The Committee further finds that improvements to the PRC's space launch capability increases the PRC's ability to use space for military reconnaissance, communications, and meteorology. The PRC's enhanced ability to use space in turn may pose challenges to U.S. national security interests and capabilities.

The perfection of a flight-worthy PRC Smart Dispenser is an example of the pulling effect leading to improved space launch services inherent in U.S. use of such services. The PRC had indigenous capability to develop a Smart Dispenser prior to Motorola's request for proposals for the Iridium project. Undertaking this project resulted in a flight-worthy dispenser. Analysts differ as to the military significance of this development.

The Committee found that decisions in 1992 and 1996 transferring licensing jurisdiction over commercial satellites from the State Department to the Commerce Department emphasized commercial interests over national security and other concerns. The 1992 decision shifted jurisdiction over the export of commercial satellites without militarily significant characteristics from the State Department to the Commerce Department. This action reduced the ability of the State and Defense Departments to block such exports on national security grounds. * * * In 1996, jurisdiction over the export of all remaining commercial satellites was transferred to Commerce.

The 1996 decision had the additional consequence of completing the process of removing commercial satellites from categories of goods that would not be exported when the U.S. government imposed Missile Technology Control Regime (MTCR) Category II sanctions. This step, at least in part, reflected industry pressure since 1992 to bring about such a policy change.

* * * * * * *

The transfer of the export of commercial satellites to Commerce Department jurisdiction affected U.S. national security. Some believe the national security was enhanced by having the PRC use U.S. satellites and by maintaining strong international demand for our satellites. On the other hand, some believe this step diminished the impact of U.S. sanctions against the PRC for its proliferation prac-

tices, thus weakening the non-proliferation regime generally.

The Committee identified a failure by successive Administrations to provide adequate funds, staff, and training to DTSA officials responsible for monitoring U.S.-PRC satellite cooperation. As a result of confusion engendered by the 1992 decision, Defense Department monitors were not present during three satellite launch campaigns in 1993–96. Existing documents show that no monitors were present in 1997 at the fourth technical interchange meeting of the Chinastar 1 campaign. Records suggest, but do not confirm, the absence of monitors at other meetings. The Committee believes these unmonitored meetings provided the PRC opportunities to collect technical information. The Committee would be surprised if the PRC did not take advantage of such opportunities to obtain technology. The Committee recommends substantial changes in the launch monitor program.

From 1988 through today, the Intelligence Community has generated and disseminated to U.S. policymakers extensive intelligence reporting on issues relevant to export policy decisions. Such reporting covers the PRC's interest in obtaining advanced U.S. technologies, the integration of the PRC's civilian and military launch vehicle programs, PRC military modernization, and PRC missile proliferation.

The Committee found that intelligence reporting dating from at least the 1980s indicated that the PRC Government has had a strategic, coordinated effort to collect technological products and information from the U.S. Government and private companies. According to intelligence reporting, the PRC Government had devoted significant resources and effort at collecting all types of technology from American sources, whether of military or commercial value or both. Although intelligence reports detailing widespread and organized PRC efforts to collect technical knowledge were available to officials involved with the satellite export program, weaknesses in procedures and insufficient resources to support the monitoring effort detracted from the overall program.

The Committee concludes that U.S. Government officials failed to take seriously enough the counterintelligence threat during satellite launch campaigns. As a result, monitors were inadequately trained and rewarded and of insufficient number. An inadequate effort was made to ensure that employees of U.S. satellite manufacturers were trained and prepared to deal with PRC efforts to obtain U.S. know-how.

With respect to PRC efforts to influence U.S. policy, the Committee focused on the following question: "Is there intelligence information[2] that substantiates the allegation that the PRC govern-

[2] For purposes of the Committee report, "Intelligence information" includes foreign intelligence (FI) and foreign counterintelligence (FCI) as defined in Section 3 of the National Security Act and in Executive Order 12333. It does not include information obtained by law enforcement investigations (unless it was also provided as FI or FCI to law enforcement agencies by intel-

ment undertook a covert program to influence the political process in the United States through political donations, and other means, during the 1996 election cycle?"

The answer to that question, the Committee concluded, was:

> Yes. * * * [Whereas] [h]istorically, the PRC government has focused entirely on influencing the U.S. President and other Executive branch officials * * * after the Taiwanese President, Lee Tung-hui, was granted a visa to the United States in 1995, PRC officials decided that it was necessary to reassess their relationship with Congress. In response to President Lee's visit, the PRC conceived of a plan[3] to influence the U.S. political process favorably toward that country. The plan was an official PRC plan, and funds were made available for its implementation. The existence of this plan is substantiated by the body of evidence reviewed by the Committee, including intelligence reports.
>
> While the primary focus of the PRC plan was the U.S. Congress, the Committee discovered no direct evidence or information of an actual attempt to influence a particular member of Congress. However, the PRC plan to influence the U.S. political process applied to various political office holders or candidates at the local, state, and federal level.
>
> There is intelligence information indicating PRC officials provided funds to U.S. political campaigns. However, the intelligence information is inconclusive as to whether the contributions were part of the overall China Plan.
>
> During a criminal investigation into violations of the Federal Election Campaign Act (FECA), Johnny Chung, a U.S. citizen and a subject of that investigation, stated that in August 1996 he had been given $300,000 by a senior PRC official to assist in the election of President Clinton. While this statement is contrary to his previous statements, the FBI can trace only about $20,000 of the $300,000 to the Democratic National Committee, via a contribution by Chung. Most of the remaining funds went for his personal use, including mortgage payments. There is also reporting regarding contributions from other sources made to a Republican candidate for state office and a Republican state office holder. There is no intelligence information indicating that contributions had any influence on U.S. policy or the U.S. political process or that any recipients knew the contributions were from a foreign source.
>
> The intermediary between Johnny Chung and the senior PRC official was Ms. Liu Chao-ying, daughter of General Liu Hua-qing, formerly the highest ranking military officer in the PRC * * *

---

ligence agencies). However, it does include information obtained in a law enforcement investigation which was in turn provided by law enforcement agencies to intelligence agencies as FI or FCI. It does not include information collected by intelligence agencies pursuant to the authority of Section 105A of the National Security Act, unless such information also is FI or FCI. It does not include information collected by other congressional committees investigating PRC political influence as such, but it could include this information if it were also FI or FCI. Finally, it does not, insofar as is known, include information protected by Rule 6e, Federal Rules of Criminal Procedure (FRCP).

[3] The term "China Plan" was used in discussions between Congress and the executive branch to refer to the collective body of information describing these efforts by the PRC.

2. PRC Nuclear Espionage, Department of Energy Security and Counterintelligence Matters, and the Wen Ho Lee Case

The Committee has jurisdiction over counterintelligence matters government-wide, including the Department of Energy (DOE) Office of Counterintelligence. From March 1999 through September 2000, the SSCI held 16 hearings on the Kindred Spirit investigation into the loss of W–88 nuclear warhead information to the PRC, the Intelligence Community damage assessment of PRC nuclear espionage, security and counterintelligence problems at the Department of Energy, DOE reorganization, the conduct of the investigation and prosecution of Wen Ho Lee for downloading and retaining classified nuclear weapons information, the resulting plea agreement between Lee and the U.S. Government, and other related matters. Witnesses included Attorney General Janet Reno, Energy Secretary Bill Richardson, FBI Director Louis Freeh, DCI George Tenet, former Energy Secretaries James Watkins, John Herrington, and Federico Pena, and the directors of the Los Alamos, Lawrence Livermore, and Sandia national laboratories. Committee members also met with National Security Advisor Sandy Berger to discuss the Administration's response to PRC nuclear espionage.

Committee Members and staff traveled to Los Alamos National Laboratory, meeting with dozens of lab officials ranging from the lab director and senior staff to scientists and computer personnel. Staff also conducted extensive interviews with the Albuquerque FBI field office and the Assistant U.S. Attorney for New Mexico, and traveled to Lawrence Livermore and Sandia national labs to interview lab and local FBI field office personnel.

Committee staff interviewed five former Secretaries of Energy and two former Deputy Secretaries of Energy, and held dozens of interviews, briefings, and meetings with current and retired senior CIA, FBI, DOE, and NSC officials, including the National Intelligence Officer for Strategic Programs, the CIA's Deputy Director for Operations, the FBI Assistant Director/National Security Division, the Director of Energy Intelligence, the former CIA Deputy Director for Intelligence, and the former National Intelligence Officer for Special Activities.

Committee staff compiled a detailed, all-source chronology of DOE counterintelligence and security problems, PRC espionage against the national laboratories, and the related DOE and FBI investigations.

Although the Committee has jurisdiction only over the counterintelligence and intelligence functions of the Department of Energy, the Senate-passed version of the Intelligence Authorization Act for Fiscal Year 2000 contained provisions (Title IX) providing for a wide-ranging reorganization of the Department to address numerous security, counterintelligence, and management shortcomings identified by the SSCI, the House Select Committee on U.S. National Security and Military/Commercial Concerns with the Peoples' Republic of China (the "Cox Committee"), and the President's Foreign Intelligence Advisory Board (the "Rudman Report"). Title IX was dropped by the Conference Committee after a similar reorganization plan was enacted as part of the National Defense Authorization Act for Fiscal Year 2000. As described elsewhere in this report the Committee also adopted legislation amending the Foreign Intelligence Surveillance Act and other counterintelligence

statutes to address issues that arose in the course of the Kindred Spirit and other investigations.

Meanwhile, the Committee has continued its oversight over the Department of Energy's Counterintelligence and Intelligence programs. The Committee continues to monitor closely the Department's implementation of Presidential Decision Directive–61 (PDD) enhancing counterintelligence capabilities at DOE, the DOE counterintelligence implementation plan, and the provisions of the National Defense Authorization Act for Fiscal Year 2000 to ensure that the Department follows through on these and other long-overdue reforms.

3. Deutch Mishandling of Classified Material

On December 17, 1996, officials of the Central Intelligence Agency (CIA) discovered classified information on the unclassified home computer of former Director of Central Intelligence (DCI) John M. Deutch. The resulting CIA security investigation, which began in January 1997, revealed that Mr. Deutch routinely had placed highly classified information on unclassified computers with Internet access.

Key steps in the 1997 security investigation of Mr. Deutch's actions were not taken, and the CIA Inspector General (IG) did not begin its own investigation until February 1998 after becoming aware that the security investigation was incomplete. On July 13, 1999, the CIA IG issued its report of investigation, which was later released in unclassified form at the Committee's request.

The SSCI initiated its own inquiry into the Deutch matter in February 2000 after becoming aware that the CIA had not actively pursued the recommendations contained in the CIA IG's report of investigation. Using the CIA IG report as foundation, the Committee sought to resolve remaining unanswered questions through more than 60 interviews with current and former Intelligence Community and law enforcement officials and a review of thousands of pages of documents. The Committee held five hearings on this topic and invited the following witnesses: CIA IG Britt Snider, Mr. Deutch, former CIA General Counsel Michael O'Neil, former CIA Executive Director Nora Slatkin, Executive Director David Carey, and DCI George Tenet. O'Neil exercised his Fifth Amendment right not to testify before the Committee. In addition, former Senator Warren Rudman, Chairman of the President's Foreign Intelligence Advisory Board, briefed the SSCI on the findings of the Board's report on the Deutch matter.

The Committee confirmed that Mr. Deutch's unclassified computers contained summaries of sensitive U.S. policy discussions, references to numerous classified intelligence relationships with foreign entities, highly classified memoranda to the President and documents imported from classified systems. 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 that he failed in this responsibility. Mr. Deutch, whose conduct should have served as the highest example, instead displayed a reckless disregard for the most basic security practices required

of thousands of government employees throughout the CIA and other agencies of the Intelligence Community.

The Committee believes further that in their response to Mr. Deutch's actions, Director Tenet, Executive Director Slatkin, General Counsel 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 committees were not notified of the security breach by Mr. Deutch until more than 18 months after its discovery.

The Committee determined that there were gaps in existing law that required legislative action. Current law required 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. In the Intelligence Authorization Act for Fiscal Year 2001, the Committee initiated a change in the Central Intelligence Agency Act of 1949 to broaden the notification requirement. The new notification requirements include former DCls, all current and former officials appointed by the President and confirmed by the Senate, the Executive Director, and the Deputy Directors for Operations, Intelligence, Administration, and Science and Technology. In addition, the Inspector General must notify the committees whenever one of the designated officials is the subject of a criminal referral to the Department of Justice.

The CIA IG's July 1999 report contained three recommendations: review Mr. Deutch's continued access to classified information; establish a panel to determine the accountability of current and former CIA officials with regard to the Deutch matter; and advise appropriate CIA and Intelligence Community components of the sensitive information Mr. Deutch stored in his unclassified computers. DCI Tenet responded to the IG report by indefinitely suspending Mr. Deutch's security clearances and instructing Executive Director Carey to form an accountability board and to notify Intelligence Community components regarding their equities.

The Executive Director established an Agency Accountability Board in September 1999, but its first meetings were in November 1999 and subsequent sessions were not held until January 2000. Ultimately, the Deputy Director of Central Intelligence decided that the final product of the accountability board was inadequate. At his request, the President's Foreign Intelligence Advisory Board conducted an independent inquiry and its conclusions were provided to the President and the Deputy Director.

During a Committee hearing in February 2000, DCI Tenet admitted that the CIA had not initiated a damage assessment on the possible compromise of the Deutch material. Executive Director Carey advised Committee staff that the failure to pursue a damage assessment in August 1999 resulted from a miscommunication. This mistake was discovered in late 1999, but was not corrected until after the Committee wrote the DCI in February 2000 requesting a damage assessment be initiated. A formal Intelligence Community-wide damage assessment is still ongoing at this time.

4. USS Cole

The USS *Cole* was attacked in Aden, Yemen on October 12, 2000. Seventeen sailors were killed and 39 were wounded. The Committee immediately began efforts to determine whether intelligence

information, analysis, and warning had been available that might have prevented that attack. The SSCI staff is conducting a comprehensive review of all available intelligence information leading up to the attack on the *Cole.* An initial review indicates that the collection and dissemination of terrorism-related information was timely and effective. A review is ongoing to determine if enhancements to the analysis and warning processes could make the intelligence information more effective in supporting commanders in the field.

C. COMMUNITY ISSUES

1. Activities of the CIA in Chile

Section 311 of P. L. 106–120, the Intelligence Authorization Act for Fiscal Year 2000, directed the DCI to submit a report to the Congress describing the activities of the Intelligence Community in Chile around the time of the 1973 assassination of President Salvador Allende and the subsequent accession to power of General Augusto Pinochet. The report also was to focus on human rights violations committed by the Pinochet regime. The DCI submitted a classified version of the report to the Committee on September 7, 2000, and an unclassified version on September 18, 2000. The report provides insight into the implementation of the U.S. policy of seeking to block Allende from coming to power. It is an important historical record not only of the role of the Intelligence Community in this effort, but also of the policy making mechanisms used to approve that role. In the report the CIA acknowledges earlier Presidentially-authorized covert actions designed to block Allende from coming to power, including support for coup plotters in 1970, but makes it clear that there was no comparable involvement in the 1973 coup.

2. Oversight of Intelligence Community Inspectors General

During the 106th Congress, the Committee continued to monitor the activities of the Inspectors General (IGs) of the Intelligence Community. This oversight included: review of over 150 IG products, to include audit reports, inspection reports, reports of investigation, and semi-annual reports of IG activities; numerous visits to IG offices for updates on plans and procedures; and attendance at several IG conferences. In addition to a number of Committee hearings on issues reviewed by the Intelligence Community IGs, staff conducted a number of briefings with Community program and IG personnel in order to follow up on the status of IG recommendations. Examples include employee grievances, management of operational activities, contracting procedures, employee recruitment and security processing, CIA's Working Capital Fund, and effective use of resources on new technology.

The Committee also adopted report language regarding the administrative Inspectors General at the NRO, the NSA, the NIMA, and the DIA. The Committee directed the Directors of these agencies to take the appropriate steps to create a separate budget line item and personnel authorization for their respective administrative IG offices, and to ensure that the IG has all the authorities required to hire and retain staff that collectively possess the variety and depth of knowledge, skills, and experience needed to ac-

complish, efficiently and effectively, the Office of Inspector General's mission. The Committee requested that the Directors provide a written response on the status of these initiatives.

The Committee also took steps to improve its oversight of the Inspectors General from the NRO, NIMA, NSA, and DIA by requesting an annual report that details their request for fiscal and personnel resources, and the plan for their use. This report will include the programs and activities scheduled for review during the fiscal year, comments on the office's ability to hire and retain qualified personnel, any concerns relating to the independence and effectiveness of the IG's office, and an overall assessment of the Agency's response to the IG's recommendations during the previous year.

3. Classified Information Procedures Act (CIPA)

The 1980 Classified Information Procedures Act (18 U.S.C. App.) has proven to be a very successful mechanism for enabling prosecutions that involve national security information to proceed in a manner that is both fair to the defendant and protective of the sensitive national security intelligence information. Before CIPA, the United States Government occasionally had to make the difficult decision of either dismissing a criminal case or proceeding in the face of the risk that classified information might be made public. Neither alternative was in the best interests of the intelligence or law enforcement agencies—nor, more importantly, in the interests of the American people. The CIPA provides pre-trial procedures for the court to resolve in camera and ex parte these issues in a manner that protects both the national security and the defendant's right to a fair trial. The government has the option of an immediate appeal of any adverse rulings and, if the issues cannot be resolved in a manner that protects national security, may then make informed decisions on whether to proceed or to dismiss some or all of the charges.

In a criminal case in which classified information is at issue—for example, espionage and terrorism prosecutions—there are specific agencies in which the information originated and whose equities are most directly implicated by the decisions made by the U.S. Government in the case. The head of that agency is responsible for protecting the information and, accordingly, will have a strong interest in the key decisions made by the prosecutors as the case develops. Although all litigation decisions must rest ultimately with the Department of Justice, it is the head of the affected agency, in most cases the Director of Central Intelligence, who will be able to provide the perspective in the decision-making process on the risks associated with public release of classified information at trial. The DCI's expertise will assist the prosecutors in their goal of not doing more harm to the national security during the case than was caused by the defendant's alleged criminal conduct.

Accordingly, Section 607 of the Intelligence Authorization Act for Fiscal Year 2001 (Public Law 106–567) amends CIPA to codify existing practice followed by many Department of Justice prosecutors. Section 607 requires the Assistant Attorney General for the Criminal Division and the United States Attorney, or their designees, to provide regular briefings to the head of the agency that originated the classified information at issue in the case. These briefings will

begin as soon as practicable and appropriate, consistent with rules governing grand jury secrecy, and will continue thereafter, as needed, to keep the agency head fully and currently informed. The purpose of the briefings is to make sure that the agency head understands the parameters and benefits of the CIPA procedures. In addition, the agency head will have an opportunity at various stages of the case to make his or her views known to the prosecutors concerning whether the case is proceeding in such a way that sources and methods are receiving adequate protection.

4. POW/MIA analytic capability in the Intelligence Community

The Committee has expressed serious concern about the Administration's accounting for Navy Lieutenant Commander "Scott" Speicher, who was shot down over Iraq on the first night of the Gulf War. A subset of these concerns relates to the lack of an adequate analytical capability within the Intelligence Community for Prisoners of War/Missing in Action (POW/MIA) issues.

The January 1993 Report of the Senate Select Committee on POW/MIA Affairs concluded that the Defense Intelligence Agency's POW/MIA Office had historically over-classified, poorly coordinated, and failed to adequately follow-up on reports. The report found a "mindset to debunk [POW] live-sighting reports."

As described elsewhere in this report, the Senate Select Committee on Intelligence conducted an inquiry into the Intelligence Community's input to support the U.S. Government's decision to list LCDR Speicher's status as killed in action. During the later part of the 105th Congress, at the request of the SSCI, the Director of Central Intelligence produced a chronology of the Speicher case. This chronology of events enabled informed judgements about questions of policy, process, and facts. Furthermore, the chronology highlighted to the Committee that a POW/MIA analytic shortfall existed within the Intelligence Community. The Committee judged that the shortfall stemmed, at least in part, from the Secretary of Defense's 1993 decision effectively to eliminate the Intelligence Community's only POW/MIA analytic capability.

The impact of this organizational change was first addressed by the Committee in a 1997 staff inquiry into the Intelligence Community's input that formed the basis for the 1996 Presidential determination regarding Vietnam's accounting for American POW/MlAs. As a result, the 1998 Defense Authorization Act directed the Director of Central Intelligence to take responsibility for all POW/MIA intelligence-related analytic matters. The shortfall in POW/MIA analytic capability surfaced again in February 2000, when the Committee received a joint CIA and Department of Defense Inspectors General review of the 1998 National Intelligence Estimate on POW/MIA matters. This report highlighted significant deficiencies in POW/MIA analysis specifically related to intelligence.

As a result, the Committee, in Section 307 of the Intelligence Authorization Act for Fiscal Year 2001 (P.L. 106–567), directed that the Director of Central Intelligence establish and maintain an analytic capability within the Intelligence Community with responsibility for supporting activities related to prisoners of war and missing persons.

5. Counterdrug Intelligence Plan

On February 12, 2000, the President issued the General Counterdrug Intelligence Plan and established the Counterdrug Intelligence Executive Secretariat. The Plan fulfilled 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 (P.L. 105–107). These two provisions required the Director of the Office of National Drug Control Policy to submit "a plan to improve coordination and eliminate unnecessary duplication among the counterdrug intelligence centers and counterdrug activities of the Federal Government," and specifically to report on efforts to structure the National Drug Intelligence Center in order to "effectively coordinate and consolidate strategic drug intelligence."

The Senate version of the Intelligence Authorization Act Fiscal Year 2001 included a provision (Section 308) to waive two existing prohibitions and authorize executive branch agencies to contribute appropriated funds for the purpose of supporting the Counterdrug Intelligence Executive Secretariat. This provision was dropped by the conference committee after similar language was signed into law as part of a supplemental appropriations act. The Committee's report language, however, requires the executive branch to report annually on the activities of the Counterdrug Intelligence Executive Secretariat.

The Committee has placed, 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 in the U.S. and its devastating societal consequences. Intelligence is critical to effective source country programs, interdiction actions, and law enforcement investigations.

6. Judicial Review Commission on Foreign Asset Control

Title VIII of the Intelligence Authorization Act for Fiscal Year 2000 comprised the Foreign Narcotics Kingpin Designation Act. Using the authorities of the International Emergency Economic Powers Act as previously applied to Colombian drug traffickers as a model, this legislation established a regime for identifying, designating, and sanctioning international drug trafficking organizations and their leadership. The Act requires the President to designate individuals as significant foreign narcotics traffickers. These individuals are then subject to sanctions, including the blocking of assets in the United States. The Act also provides for the blocking of assets of foreign persons who materially assist or support the traffickers, or who are determined to be acting on behalf of the traffickers.

Section 810 of Title VIII created a commission to review judicial, regulatory, and administrative authorities used to block assets of foreign persons and to provide the Congress with an evaluation of remedies available to any U.S. person affected by the blocking of assets of foreign persons. The fundamental question that the Commission was asked to address was whether provisions in the Act provide constitutionally adequate remedies to U.S. persons to challenge agency designations and blocking actions. The Judicial Review Commission submitted its final report to Congress on January

23, 2001. The report set forth detailed legal analysis and fact-finding activities of the Commission in support of the findings and recommendations that had been submitted to the Committee on an interim basis on December 4, 2000. Among the recommendations contained in the report was an endorsement of the position of the Committee, and the Senate, that judicial review should be permitted for decisions under the Kingpin Act. In addition, the report made a number of recommendations regarding the administration and enforcement of sanctions programs by the Office of Foreign Asset Control.

7. National Commission for the Review of the National Reconnaissance Office

During the conference on the Intelligence Authorization Act for Fiscal Year 2000, the Senate and House Committees agreed to initiate an independent review of the National Reconnaissance Office. The review would consider how the NRO can provide the most capable and cost efficient satellite collection systems possible to ensure that national policy makers and military leaders continue to receive timely intelligence information. In particular, Intelligence Committee Members wanted to evaluate the impact on satellite collection capabilities of dramatic changes in technology, coupled with significant shifts in the global threat environment over the past decade. These factors could seriously affect the ability of NRO satellites to continue to provide timely intelligence information.

The Commission was comprised of eleven members: two from the Senate, two from the House of Representatives, six from the private sector, and the Deputy Director of Central Intelligence for Community Management. The Director of the NRO was an ex-officio member.

The Committees tasked the Commission to review the NRO's roles and missions, organizational structure, and contractor relationships; the technical skills of the NRO employees; the use of commercial imagery; launch and supporting services; and acquisition authorities. The Commission also was asked to review the NRO's relationship with other agencies and Government departments. The Commission's final report, with recommendations, was delivered to the Intelligence and Armed Services Committees of the Senate and House of Representatives. The Committee is reviewing these recommendations. The Committees also tasked the Director of Central Intelligence and Secretary of Defense to provide an assessment of the report to the Intelligence Committees.

D. AUDITS

The Committee's audit staff was created in 1988 to provide "a credible independent arm for Committee review of covert action programs and other specific Intelligence Community functions and issues." During the 106th Congress, the staff of three full-time auditors led, or provided significant support to, the Committee's review of a number of administrative and operational issues relating to the agencies of the Intelligence Community. In addition, the audit staff completed three in-depth reviews of specific intelligence programs or issues. These reviews included the following:

1. Review of the National Imagery and Mapping Agency (NIMA)

The audit examined NIMA's charter and legal authorities, financial management system, personnel and facilities, procedures for acquisition and property management, Office of Inspector General, and information security practices. The audit staff was encouraged by NIMA's progress in each of these areas. The Agency has used its status as a new organization to create innovative programs, particularly in the areas of contracting and personnel management. The resulting audit report contained recommendations aimed at streamlining the NIMA's administrative processes, strengthening its position within the Intelligence Community, and resolving open issues remaining from the creation of the NIMA in 1996.

2. Covert action

The staff examined a covert action program, including the program's operations, financial obligations and expenses, and future plans. The audit found a well-managed program, and the resulting report made a recommendation to the Committee regarding the appropriate funding level for the program.

To enhance the Committee's understanding of this intelligence target, the audit also included a review of the Intelligence Community's collection and analytic capabilities against a particular country. The staff found weaknesses similar to those identified for other targets and, as such, made a recommendation for systemic review by the Assistant Director of Central Intelligence for Analysis and Production.

3. Other

The audit staff has recently begun a review of the strategic plan of the Central Intelligence Agency's Directorate of Operations.

The audit staff conducted over 30 interviews and reviewed voluminous documentation related to the Committee's inquiry into former Director of Central Intelligence John Deutch's mishandling of classified information, and drafted and coordinated the Deutch report for the Committee's approval. The Deutch report was provided to the DCI and Department of Justice.

In addition to these major projects, the audit staff completed portions of the Committee staff's investigations of satellite and missile technology transfers to the People's Republic of China, and counterintelligence and security issues at the Department of Energy's National Laboratories. The team also worked to ensure the Intelligence Community's Inspectors General have the necessary independence, funding, management structure, and professional staff to adequately monitor the activities of their respective agencies.

E. TECHNICAL ADVISORY GROUP REPORTS

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 and 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 identify problems, solutions, and opportunities posed by advances in technology.

In the 106th Congress, the Committee continued to draw upon the TAG's world-class expertise, and to incorporate the TAG's findings as appropriate into the Committee's budgetary and legislative recommendations. The Committee is grateful to the TAG members for their contribution to our nation's security.

1. Signals intelligence—Rebuilding the NSA

The NSA has responsibility for collecting signals intelligence (SIGINT) from electronic signals worldwide. 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, we have failed to invest in the infrastructure and organizational changes required to keep pace with revolutionary developments in the global telecommunications system.

In 1998, the TAG completed a study of the NSA based on a thorough review of current and planned operations as well as research and development programs.

The conclusions of the TAG's 1998 report were extremely 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 was found to be in serious doubt due to 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. To address these problems, the TAG recommended new business practices coupled with additional resources to finance this recovery.

A follow-up TAG review completed in Spring 2000 sounded a note of optimism, noting that the NSA Director, in November 1999, had initiated an aggressive and ambitious modernization effort designed to transform the NSA and sustain it as a national asset. This transformation—which gained additional impetus from the NSA computer outage in January 2000—includes organizational and business strategies that promise to transform the way the NSA conducts its missions. The Committee was 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. The Committee determined that 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.

Rebuilding the NSA is the Committee's top priority. To provide the additional resources necessary, the Committee has had to make tough choices. Inadequate NFIP spending has left little flexibility to meet the challenges faced by the NSA, but the Committee concluded that the crisis demanded immediate attention and warranted shifting resources in order to stave off a steady and inevitable degradation of the NSA's unique and invaluable capabilities. In its budget recommendations for Fiscal Years 2000 and 2001, the Committee has made a down payment on this investment.

At the same time, the Committee knows that money alone will not 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 is determined to work with the Director to improve his ability to provide centralized direction across the SIGINT infrastructure as he implements his modernization strategy.

2. Human intelligence—Bringing technology in from the cold

In 1998, the Committee asked the TAG to review the status of the Intelligence Community's human intelligence (HUMINT) capabilities. The TAG concluded that while human intelligence collection will play an increasingly important role in defending U.S. national security interests, the CIA Directorate of Operations (DO) lagged in integrating the technical knowledge and training needed to become a more technologically oriented, technology-savvy, and technology-responsive organization. The HUMINT TAG recommended that:

> The Intelligence Community develop a comprehensive plan that recognizes and adapts to the rapidly changing and technically sophisticated world that now confronts the HUMINT collector;
>
> The DO continue development of a strategic vision and implementation plan that focuses on missions rather than functions and emphasizes elements that integrate science and technology into its mission solutions; and
>
> Additional funding be provided to move toward a set of highly advanced capabilities and techniques that will enable the DO to practice high-technology, clandestine, intelligence collection in the first half of this decade.

In response to the TAG's 1998 recommendations and related Committee guidance, the CIA made key changes in an effort to take advantage of opportunities provided by technological innovation. In 2000, the Committee asked the TAG to assess the progress that the Intelligence Community had made in undertaking the substantial changes recommended in 1998, and incorporated the TAG's findings in its budgetary and other actions on the Fiscal Year 2001

Intelligence Authorization Act. The Committee will closely monitor the DO's efforts to make better use of technological innovations.

3. Measurement and signature intelligence (MASINT)—Funding and organizing to realize potential

In 1999, the TAG reviewed the Intelligence Community's capabilities to collect MASINT, in particular whether MASINT was meeting its potential in the areas of management, funding, technology development, operations, and integration with other intelligence disciplines.

The TAG found that MASINT can significantly strengthen collection against many emerging threats, and potentially become the Intelligence Community's most valuable source of technical intelligence in the 21st Century. The need for an improved MASINT capability is driven by global advances in technology and in our adversaries' ability to conduct denial and deception against traditional intelligence collection methods. The MASINT panel concluded that MASINT technologies can—if aggressively developed and integrated with other intelligence disciplines—add to and complement the value of current collection capabilities, but that realizing this potential requires changes in the current approach to MASINT technology development.

The Committee has allocated a significant amount of additional funds over the last two years to bolster MASINT capability. The Committee also directed the Director of Central Intelligence, in coordination with the Secretary of Defense, to conduct a study of the utility and feasibility of various options for improving the management and organization of MASINT, including (1) the option of establishing a centralized tasking, processing, exploitation, and dissemination facility for measurement and signature intelligence, (2) options for recapitalizing and reconfiguring the current systems for measurement and signature intelligence, and (3) the operation and maintenance costs of the various options.

4. Imagery intelligence (IMINT)—Keeping the customers satisfied

In 1999, the Committee asked the Technical Advisory Group to review three key areas in Intelligence Community management of IMINT. The Committee asked the TAG to focus on the Future Imagery Architecture program, the imagery requirements process, and the broad functions of tasking, processing, exploitation, and dissemination of imagery intelligence products.

In April 1999, the TAG briefed Committee members on its findings and recommendations. The report highlighted the tensions between varying imagery requirements from the tactical, theater, strategic, and national level intelligence customers, and the difficulty in satisfying these often conflicting taskmasters. One option to address these proliferating demands is to develop dedicated imagery systems designed to meet the limited requirements of a particular customer, which may be more cost-effective than designing large-scale systems to meet unlimited requirements. The TAG found that the Intelligence Community has not analyzed these issues with adequate rigor.

The TAG report to the Committee also emphasized the significant gap between imagery collection requirements and the ability of the Intelligence Community to process, exploit, and disseminate

imagery products. Although some actions had been taken by the Intelligence Community to close the gap, there are still many serious problems. This issue is addressed at length in the section of this report dealing with tasking, processing, exploitation, and dissemination of intelligence.

IV. CONFIRMATIONS

A. JAMES M. SIMON, JR., ASSISTANT DIRECTOR OF CENTRAL INTELLIGENCE FOR ADMINISTRATION

On February 4, 1999, the Committee held public hearings on the nomination of James M. Simon, Jr. to be the Assistant Director of Central Intelligence for Administration. Mr. Simon, a career CIA officer was nominated by the President to the position on January 6, 1999. (The Senate-confirmable position of Assistant Director for Administration was one of several positions created by the Intelligence Authorization Act for Fiscal Year 1997 in response to the 1996 Brown Commission, which made recommendations regarding the effectiveness and efficiency of the Intelligence Community.) In addition to his administrative responsibilities at the CIA, the Assistant Director for Administration serves as the deputy to the Deputy Director of Central Intelligence for Community Management.

Mr. Simon's nomination was considered favorably by the Committee on February 26, 1999. The Senate considered and approved his nomination on March 2, 1999 by voice vote. A full transcript of the nomination hearing was published in S. Hrg. 106–394, a Government Printing Office publication.

B. JOHN E. MCLAUGHLIN, DEPUTY DIRECTOR OF CENTRAL INTELLIGENCE

On July 27, 2000, the Committee held a closed hearing on the nomination of John E. McLaughlin to be the Deputy Director of Central Intelligence (DDCI). McLaughlin, an expert in European, Russian, and Eurasian affairs, was nominated by the President on July 13, 2000. The Deputy Director of Central Intelligence is required by the National Security Act of 1947 to assist the Director in carrying out his functions and to serve in his place in his absence.

Mr. McLaughlin's nomination was considered favorably by the Committee on July 27, 2000, by a vote of 15–0. The Senate approved his nomination on October 18, 2000 by voice vote.

V. SUPPORT TO THE SENATE

The Committee undertook a number of activities to support the Senate's deliberations. In addition to its unclassified reports, the Committee has sought to support Senate deliberations by inviting the participation of Members outside the Committee in briefings and hearings on issues of shared jurisdiction or interest. The Committee has prepared, and made available for the Senate, compendia of intelligence information regarding topics relevant to current legislation. Members outside the Committee have frequently sought and received intelligence briefings by members of the Committee staff. Members have also requested and received assistance in re-

solving issues with the actions of an element of the Intelligence Community. Finally, the Committee routinely invites staff from other Committees to staff-level briefings on intelligence issues of common concern.

VI. Appendix

A. SUMMARY OF COMMITTEE ACTIVITIES

1. Number of meetings

During the 106th Congress, the Committee held a total of 99 on-the-record meetings and hearings. There were fifty-seven (57) oversight hearings and eight (8) business meetings. Twelve (12) hearings were held on the budget, including the Conference sessions with the House. Two (2) nomination hearings were held.

Additionally, the Committee held seventeen (17) on-the-record briefings and over two hundred fifty (250) off-the-record briefings.

2. Bills and resolutions originated by the Committee

S. Res. 139—An original resolution authorizing expenditures by the Select Committee on Intelligence.

S. 1009—Intelligence Authorization Act for Fiscal Year 2000.

S. 2507—Intelligence Authorization Act for Fiscal Year 2001.

3. Bills referred to the Committee

S. 1902—Japanese Imperial Army Disclosure Act.

S. 2089—Counterintelligence Reform Act of 2000.

4. Publications

Senate Report 106–3—Committee Activities, Special Report of the Select Committee on Intelligence, January 7, 1997–October 21, 1998 (February 3, 1999).

Senate Report 106–48—Report to accompany S. 1009, FY 00 Intelligence Authorization Bill (May 11, 1999).

Senate Print 1067–25—Report on Impacts to U.S. National Security of Advanced Satellite Technology Exports to the People's Republic of China (PRC), and Report on the PRC's Efforts to Influence U.S. Policy (May 1999).

Senate Hearing 105–1056—Nomination of Joan A. Dempsey to be Deputy Director of Central Intelligence for Community Management (May 21, 22, 1998).

Senate Hearing 106–394—Nomination of James M. Simon, Jr., to be Assistant Director of Central Intelligence for Administration (February 4 and 26, 1999).

Senate Hearing 105–1054—Nomination of L. Britt Snider to be Inspector General, Central Intelligence Agency (July 8 and 14, 1998).

Senate Hearing 105–1057—Investigation of Impacts to U.S. National Security From Advanced Satellite Technology Exports to China and Chinese Efforts to Influence U.S. Policy (June 10 and July 15, 1998).

Senate Report 106–279—Report to Accompany S. 2507, FY 01 Intelligence Authorization Bill (May 4, 2000).

Senate Hearing 106–452—Joint Hearing Before the Committee on Energy and Natural Resources, the Committee on Armed Services, the Committee on Governmental Affairs, and the Select Com-

mittee on Intelligence on The President's Foreign Intelligence Advisory Board Report on DOE (June 22, 1999).

Senate Hearing 106–580—Current and Projected National Security Threats to the United States (February 2, 2000).

Senate Hearing 106–592—Department of Energy Counterintelligence, Intelligence and Nuclear Security Reorganization (June 9, 1999).

Senate Report 106–352—Report to Accompany S. 2089, The Counterintelligence Reform Act of 2000 (July 20, 2000).

Report 106–969—Conference Report to Accompany H.R. 4392, FY 01 Intelligence Authorization Bill (October 11, 2000).

○