CHAPTER 4

INTRODUCTION

On 18 March 1999, the President requested the President's Foreign Intelligence Advisory Board (PFIAB), chaired by former Senator Warren Rudman, to review the security threat at DOE's nuclear weapons laboratories and the measures that have been taken to address that threat. On 15 June 1999, the PFIAB presented its report, *Science at Its Best—Security at Its Worst* (the "Rudman report"), to the President. The report found that DOE "is a dysfunctional bureaucracy that has proven it is incapable of reforming itself." The report stated that the "nuclear weapons and research functions of DOE need more autonomy, a clearer mission, a streamlined bureaucracy, and increased accountability."

Following its extensive 1999 review of DOE security and counterintelligence (CI) problems, the House Intelligence Committee continued its oversight over DOE's CI and intelligence programs. The Committee closely monitored DOE's implementation of Presidential Decision Directive-61 (PDD-61)—the DOE Counterintelligence Implementation Plan and the National Defense Authorization Act of Fiscal Year 2000—to ensure that DOE followed through on these and other long-overdue reforms. The Committee was disappointed that, in DOE's initial CI inspections of the major weapons laboratories, only one lab—Lawrence Livermore National Laboratory—received a satisfactory rating. The Committee was also concerned that neither the DOE Director of CI, the DCI, nor the FBI Director could certify to Congress that DOE's foreign visitors program complied with applicable DOE directives and PDD and similar requirements and did not pose an undue risk to US national security.

Congressional concern over security at the nuclear weapons laboratories increased again in June 2000 when several computer hard drives containing nuclear weapons information were lost at Los Alamos. The hard drives were later found behind a photocopier close to the vault where the drives were stored. The FBI, which had been investigating the disappearance of the hard drives, believed that one or possibly more scientists took the drives from the vault in April and misplaced them. Fearful of possible punishment for a security lapse, the scientist or scientists engaged in the coverup—put the drives behind the copier.

During the previous seven years, new CI mechanisms to address economic and industrial espionage were created and procedures implemented to improve coordination among intelligence, CI, and law enforcement agencies. It was felt that these measures had considerably strengthened the US Government's ability to counter the foreign intelligence threat. However, there was a difference of opinion.

On 8 March 2000, during a closed hearing before the Senate Select Committee on Intelligence (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 CI structures and capabilities to address emerging, as well as traditional, CI issues. The drafters of the CI 21 plan found current US CI capabilities to be "piecemeal and parochial," and recommended adoption of a new CI philosophy—described as more policy-driven, prioritized, and flexible, with a strategic, national-level focus—as well as a restructured national CI system. CI 21 proposed significant changes in the way the US Government approaches and organizes itself to meet the threat of foreign espionage and intelligence gathering.

Congress noted that the FBI's National Infrastructure Protection Center (NIPC)—charged with detecting, preventing, and responding to cyber and physical attacks on US critical

infrastructures—and the new Office of National Counterintelligence Executive (NCIX) had similarities in mission and interagency focus. This prompted Congress to suggest that both these offices be co-located at one site. They directed a joint written assessment be done by the NCIX Executive, the DCI, and the FBI Director and provide to the intelligence oversight committees. This assessment, of the desirability and feasibility (including a budgetary assessment) of colocating the NIPC and NCIX at one site, separate and apart from CIA, FBI, and Department of Defense facilities, was due by sometime in late 2002.

The Fiscal Year 2001 Intelligence Authorization Bill had provisions to establish criminal penalties for the unauthorized disclosure of properly classified information. Previous legislation established penalties only for disclosure of specific types of classified material—codes and cryptographic devices and information related to nuclear programs. After some debate about the provision, President William Clinton vetoed the bill on 4 November 2000. Another version of the FY2001 authorization bill without the disclosure provision was enacted on 27 December 2000. Proponents of the provision tried again after President George W. Bush came into office, but nonsupport from the White House again killed the provision.

Leaks continue to plague the government and the Intelligence Community. This was quite evident by information being made available to the media by Congress relating to the US war against terrorism following the 11 September 2001 destruction of the World Trade Center Towers in New York and part of the Pentagon by terrorists using hijacked US airlines. President Bush ordered that only a few selected members of Congress were to be briefed. Still, the media obtained classified information and published it.

The Rudman Report

(Editor's Note: The following is an edited summary of the Rudman Report.)

On 18 March 1999, President William J. Clinton requested that the President's Foreign Intelligence Advisory Board (PFIAB) undertake an inquiry and issue a report on "the security threat at the Department of Energy's (DOE) weapons labs and the adequacy of the measures that have been taken to address it."

Specifically, the President asked the PFIAB to "address the nature of the present counterintelligence security threat, the way in which it has evolved over the last two decades and the steps we have taken to counter it, as well as to recommend any additional steps that may be needed." He also asked the PFIAB "to deliver its completed report to the Congress, and, to the fullest extent possible consistent with our national security, release an unclassified version to the public."

This report, including an appendix of supporting documents, is unclassified. A large volume of classified material, which was also reviewed and distilled for this report, has been relegated to a second appendix that is available only to authorized recipients. This report examines:

- The 20-year history of security and counterintelligence issues at the DOE national laboratories, with an emphasis on the five labs that focus on weapons-related research.
- The inherent tension between security concerns and scientific freedom at the labs and its effect on the institutional culture and efficacy of DOE.
- The growth and evolution of the foreign intelligence threat to the national labs, particularly in connection with the Foreign Visitor's Program.
- The implementation and effectiveness of Presidential Decision Directive No. 61, the reforms instituted by Secretary of Energy Bill Richardson, and other related initiatives.
- Additional measures that should be taken to improve security and counterintelligence at the labs.

Foreword From the Special Investigative Panel

For the past two decades, DOE has embodied science at its best and security of secrets at its worst.

Within DOE are a number of the crown jewels of the world's government-sponsored scientific research and development organizations. With its record as the incubator for the work of many talented scientists and engineers—including many Nobel prize winners—DOE has provided the nation with far-reaching advantages. Its discoveries not only helped the United States to prevail in the Cold War, but they undoubtedly will also continue to provide both technological benefits and inspiration for the progress of generations to come. The vitality of its national laboratories is derived to a great extent from their ability to attract talent from the widest possible pool, and they should continue to capitalize on the expertise of immigrant scientists and engineers. However, we believe that the dysfunctional structure at the heart of DOE has too often resulted in the mismanagement of security in weapons-related activities and a lack of emphasis on counterintelligence.

DOE was created in 1977 and heralded as the centerpiece of the federal solution to the energy crisis that had stunned the American economy. A vital part of this new initiative was the Energy Research and Development Administration (ERDA), the legacy agency of the Atomic Energy Commission (AEC) and inheritor of the national programs to develop safe and reliable nuclear weapons. The concept, at least, was straightforward: take the diverse and dispersed energy research centers of the nation, bring them under an umbrella organization with other energy-related enterprises, and spark their scientific progress through closer contacts and centralized management.

However, the brilliant scientific breakthroughs at the nuclear weapons laboratories came with a very troubling record of security administration. For example:

- Classified documents detailing the designs of the most advanced nuclear weapons were found at the Los Alamos laboratory on library shelves accessible to the public.
- Employees and researchers were receiving little, if any, training or instruction regarding espionage threats.
- Multiple chains of command and standards of performance negated accountability, resulting in pervasive inefficiency, confusion, and mistrust.
- Competition among laboratories for contracts and among researchers for talent, resources, and support distracted management from security issues.
- Sloppy accounting bedeviled fiscal management.
- Inexact tracking of the quantities and flows of nuclear materials was a persistent worry.
- Geographic decentralization fractured policy implementation, and changes in leadership regularly depleted the small reservoirs of institutional memory.

Permeating all of these issues was a prevailing cultural attitude among some in the DOE scientific community that regarded the protection of nuclear know-how with either fatalism or naivete.

In response to these problems, DOE has been the subject of a nearly unbroken history of dire warnings and attempted but aborted reforms. A cursory review of the open-source literature on the DOE record of management presents an abysmal picture. Second only to its world-class intellectual feats has been its ability to fend off systemic change. Over the last dozen years, DOE has averaged some kind of major departmental shakeup every two to three years. No President, Energy Secretary, or Congress has been able to stem the recurrence of fundamental problems. All have been thwarted time after time by the intransigence of this institution. The Special Investigative Panel found a large organization saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial. For instance, even after President Clinton issued Presidential Decision Directive 61 ordering DOE to make fundamental changes in security procedures, compliance by Department bureaucrats was grudging and belated.

Repeatedly over the past few decades, officials at DOE Headquarters and at the weapons labs have been presented with overwhelming evidence that their lackadaisical oversight could lead to an increase in the nuclear threat against the United States. Throughout its history, DOE has been the subject of scores of critical reports from the General Accounting Office (GAO), the Intelligence Community, independent commissions, private management consultants, its Inspector General, and its security experts. It has repeatedly attempted reforms. Yet the DOE's ingrained behavior and values have caused it to continue to falter and fail.

Prospects for Reforms

We believe that Secretary of Energy Richardson, in attempting to deal with many critical security matters facing the Department, is on the right track regarding some, though not all, of his changes. We concur with and encourage many of his recent initiatives, and we are heartened by his aggressive approach and command of the issues. But we believe that he has overstated the case when he asserts, as he did several weeks ago, that "Americans can be reassured: our nation's nuclear secrets are, today, safe and secure."

After a review of more than 700 reports and studies, thousands of pages of classified and unclassified source documents, interviews with scores of senior federal officials, and visits to several of the DOE laboratories at the heart of this inquiry, the Special Investigative Panel has concluded the Department of Energy is incapable of reforming itself—bureaucratically and culturally—in a lasting way, even under an activist Secretary.

The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility toward security issues, which has continually frustrated the efforts

of its internal and external critics, notably the GAO and the House Energy and Commerce Committee. Therefore, a reshuffling of offices and lines of accountability may be a necessary step toward meaningful reform, but it almost certainly will not be sufficient.

Even if every aspect of the ongoing structural reforms is fully implemented, the most powerful guarantor of security at the nation's weapons laboratories will not be laws, regulations, or management charts. It will be the attitudes and behavior of the men and women who are responsible for the operation of the labs each day. These attitudes will not change overnight, and they are likely to change only in a different cultural environment—one that values security as a vital and integral part of day-to-day activities and believes it can coexist with great science.

We are convinced that when Secretary Richardson leaves office his successor is not likely to have a comparable appreciation of the gravity of the Department's past problems nor a comparable interest in resolving them. The new secretary will have a new agenda to pursue and may not focus on DOE's previous mismanagement of national secrets. Indeed, the core of the Department's bureaucracy is quite capable of revising Secretary Richardson's reforms and may well be inclined to do so if given the opportunity.

Ultimately, the nature of the institution and the structure of the incentives, under a culture of scientific research, require great attention if they are to be made compatible with the levels of security and the degree of command and control warranted where the research and stewardship of nuclear weaponry is concerned. Yet it must be done.

Solutions

Our panel has concluded that the Department of Energy, when faced with a profound public responsibility, has failed. Therefore, this report suggests two alternative organizational solutions, both of which we believe would substantially insulate the weapons laboratories from many of DOE's historical problems and, over time, promote the building of a responsible culture. We also offer recommendations for improving various aspects of security and counterintelligence at DOE, such as personnel assurance, cyber security, program management, and interdepartmental cooperation under the Foreign Intelligence Surveillance Act of 1978.

- The weapons research and stockpile management functions should be placed wholly within a new semiautonomous agency within DOE that has a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. Useful lessons along these lines can be taken from the National Security Agency (NSA) or Defense Advanced Research Projects Agency (DARPA) within the Department of Defense or the National Oceanographic and Atmospheric Administration (NOAA) within the Department of Commerce.
- A wholly independent agency, such as the National Aeronautics and Space Administration (NASA), should be created.

There was substantial debate among the members of the panel regarding the strengths and weaknesses of these two alternatives. In the final analysis, whether to adopt or reject either of the above solutions rests in the hands of the President and the Congress, and we trust that they will give serious deliberation to the merits and shortcomings of the alternatives before enacting major reforms. We all agree, nonetheless, that the labs should never be subordinated to the Department of Defense.

With either proposal it will be important for the weapons labs to maintain effective scientific contact on unclassified scientific research with the other DOE labs and the wider scientific community. To do otherwise would work to the detriment of the nation's scientific progress and security over the long run. This argument draws on history: nations that honor and advance freedom of inquiry have fared better than those who have sought to arbitrarily suppress and control the community of science.

However, we would submit that we do not face an either/or proposition. The past 20 years have

provided a controlled experiment of a sort, the results of which point to institutional models that hold promise. Organizations such as NASA and DARPA have advanced scientific and technological progress while maintaining a respectable record of security. Meanwhile, the Department of Energy, with its decentralized structure, confusing matrix of crosscutting and overlapping management, and shoddy record of accountability, has advanced scientific and technological progress, but at the cost of an abominable record of security with deeply troubling threats to American national security.

Thomas Paine once said that, "government, even in its best state, is but a necessary evil; in its worst state, an intolerable one." This report finds that DOE's performance, throughout its history, should have been regarded as intolerable.

We believe the results and implications of this experiment are clear. It is time for the nation's leaders to act decisively in the defense of America's national security.

Bottom Line

DOE represents the best of America's scientific talent and achievement, but it has also been responsible for the worst security record on secrecy that the members of this panel have ever encountered.

With its record as the incubator for the work of many talented scientists and engineers—including many Nobel Prize winners—DOE has provided the nation with far-reaching advantages. DOE's discoveries not only helped the United States to prevail in the Cold War, they will also undoubtedly provide both technological benefits and inspiration for the progress of generations to come. Its vibrancy is derived to a great extent from its ability to attract talent from the widest possible pool, and it should continue to capitalize on the expertise of immigrant scientists and engineers. However, the Department has devoted far too little time, attention, and resources to the prosaic but grave responsibilities of security and counterintelligence in managing its weapons and other national security programs.

Findings

The preponderance of evidence accumulated by the Special Investigative Panel, spanning the past 25 years, has compelled the members to reach many definite conclusions—some very disturbing—about the security and well being of the nation's weapons laboratories.

As the repository of America's most advanced know-how in nuclear and nuclear-related armaments and the home of some of America's finest scientific minds, these labs have been and will continue to be a major target of foreign intelligence services, friendly as well as hostile. Two landmark events, the end of the Cold War and the overwhelming victory of the United States and its allies in the Persian Gulf war, markedly altered the security equations and the outlook of nations throughout the world. Friends and foes of the United States intensified their efforts to close the technological gap between their forces and those of America, and some redoubled their efforts in the race for weapons of mass destruction. Under the restraints imposed by the Comprehensive Test Ban Treaty, powerful computers have replaced detonations as the best available means of testing the viability and performance capabilities of new nuclear weapons. Research done by US weapons laboratories with high performance computers stands particularly high on the espionage hit list of other nations, many of which have used increasingly more sophisticated and diverse means to obtain US research necessary to join the nuclear club.

Reports, studies, and formal inquiries written over the past 25 years—by executive branch agencies, Congress, independent panels, and DOE have identified a multitude of chronic security and counterintelligence problems at all of the weapons labs. These reviews produced scores of stern, almost pleading entreaties for change. Critical security flaws in management and planning, personnel assurance, some physical security areas, control of nuclear materials, protection of documents and computerized information, and

counterintelligence have been continuously cited for immediate attention and resolution.

The open-source information on the weapons laboratories overwhelmingly supports a troubling conclusion: for decades their security and counterintelligence operations have been seriously hobbled and relegated to low-priority status. The candid, closed-door testimony of current and former federal officials, as well as the content of voluminous classified materials received by this panel in recent weeks, reinforce this conclusion. When it comes to a genuine understanding of and appreciation for the value of security and counterintelligence programs, especially in the context of America's nuclear arsenal and secrets, the DOE and its weapons labs have been Pollyannaish. The predominant attitude toward security and counterintelligence among many DOE and lab managers has ranged from half-hearted, grudging accommodation to smug disregard. Thus, the panel is convinced that the potential for major leaks and thefts of sensitive information and material has been substantial. Moreover, such security lapses would have occurred in bureaucratic environments that would have allowed them to go undetected with relative ease.

Organizational disarray, managerial neglect, and a culture of arrogance—at both DOE headquarters and the labs—conspired to create an espionage scandal waiting to happen. The physical security efforts of the weapons labs (often called the "guns, guards, and gates") have had some isolated shortcomings, but on balance they have developed some of the most advanced security technology in the world. However, perpetually weak systems of personnel assurance, information security, and counterintelligence have invited attack by foreign intelligence services. Among the defects, this panel found:

- Inefficient personnel clearance programs, wherein haphazard background investigations could take years to complete and the backlogs numbered in the tens of thousands.

- Loosely controlled and casually monitored programs for thousands of unauthorized foreign scientists and assignees—despite more than a decade of critical reports from the General Accounting Office, the DOE Inspector General, and the Intelligence Community.

- This practice occasionally created bizarre circumstances in which regular lab employees with security clearances were supervised by foreign nationals on temporary assignment.

- Feckless systems for control of classified documents, which periodically resulted in thousands of documents being declared lost.

- Counterintelligence programs with part-time CI officers, who often operated with little experience and minimal budgets and who employed little more than crude "awareness" briefings of foreign threats and perfunctory and sporadic debriefings of scientists traveling to foreign countries.

- A lab security management reporting system that led everywhere except to responsible authority.

- Computer security methods that were naive at best and dangerously irresponsible at worst.

Why were these problems so blatantly and repeatedly ignored? DOE has had a dysfunctional management structure and culture that only occasionally gave proper credence to the need for rigorous security and counterintelligence programs at the weapons labs. For starters, there has been a persisting lack of strong leadership and effective management at DOE.

The nature of the intelligence-gathering methods used by the People's Republic of China (PRC) poses a special challenge to the United States in general and the weapons labs in particular. More sophisticated than some of the blatant methods employed by the former Soviet bloc espionage services, PRC intelligence operatives know their strong suits and play them extremely well. Increasingly more nimble, discreet, and transparent

in their spying methods, the Chinese services have become very proficient in the art of seemingly innocuous elicitation of information. This modus operandi has proved very effective against unwitting and ill-prepared DOE personnel.

Despite widely publicized assertions of wholesale losses of nuclear weapons technology from specific laboratories to particular nations, the factual record in the majority of cases regarding the DOE weapons laboratories supports plausible inferences—but not irrefutable proof—about the source and scope of espionage and the channels through which recipient nations received information. The panel was not charged, nor was it empowered, to conduct a technical assessment regarding the extent to which alleged losses at the national weapons laboratories may have directly advanced the weapons development programs of other nations. However, the panel did find these allegations to be germane to issues regarding the structure and effectiveness of DOE security programs, particularly the counterintelligence functions.

The classified and unclassified evidence available to the panel, while pointing out systemic security vulnerabilities, falls short of being conclusive. The actual damage done to US security interests is, at the least, currently unknown; at worst, it may never be known. Numerous variables are inescapable. Analysis of indigenous technology development in foreign research laboratories is fraught with uncertainty. Moreover, a nation that is a recipient of classified information is not always the sponsor of the espionage by which it was obtained. However, the panel does concur, on balance, with the findings of the recent DCI-sponsored damage assessment. We concur also with the findings of the subsequent independent review, led by Ret. Adm. David Jeremiah, of that damage assessment.

DOE is a dysfunctional bureaucracy that has proven it is incapable of reforming itself. Accountability at DOE has been spread so thinly and erratically that it is now almost impossible to find. The long traditional and effective method of entrenched DOE and lab bureaucrats is to defeat security reform initiatives by waiting them out. They have been helped in this regard by the frequent changes in leadership at the highest levels of DOE—nine Secretaries of Energy in 22 years. Eventually, DOE's reform-minded management transitions out, either due to a change in administrations or as a result of the traditional "revolving door" management practices. Then the bureaucracy reverts to old priorities and predilections. Such was the case in December 1990 with the reform recommendations carefully crafted by a special task force commissioned by then-Energy Secretary James D. Watkins (Adm. Ret.). The report skewered DOE for unacceptable "direction, coordination, conduct, and oversight" of safeguards and security. Two years later, the new administration came in, priorities were redefined, and the initiatives all but evaporated. Deputy Secretary Charles Curtis, in late 1996, investigated clear indications of serious security and CI problems and, in response, drew up a list of initiatives. Those initiatives were dropped after he left office.

Reorganization is clearly warranted to resolve the many specific problems with security and counterintelligence in the weapons laboratories and also to address the lack of accountability that has become endemic throughout the entire Department. Layer upon layer of bureaucracy, accumulated over the years, has diffused responsibility to the point where scores claim it, no one has enough to make a difference, and all fight for more. Convoluted, confusing, and often contradictory reporting channels make the relationship between DOE headquarters and the labs, in particular, tense, internecine, and chaotic. In between the headquarters and the laboratories are field offices, which the panel found to be a locus of much confusion. In background briefings of the panel, senior DOE officials often described them as redundant operations that function as a shadow headquarters, often using their political clout and large payrolls to push their own agendas and budget priorities in Congress. Even with the latest DOE restructuring, the weapons labs are reporting far too many DOE masters.

The criteria for the selection of Energy Secretaries have been inconsistent in the past. Regardless of the outcome of ongoing or contemplated reforms, the minimum qualifications for an Energy Secretary should include experience in not only energy and scientific issues, but also national security and intelligence issues. The list of former Secretaries, Deputy Secretaries, and Under Secretaries meeting all of these criteria is very short. Despite having a large proportion (roughly 30 percent) of its budget devoted to functions related to nuclear weapons, DOE has often been led by men and women with little expertise and background in national security. The result has been predictable: security issues have been a low priority, and leaders unfamiliar with these issues have delegated decision-making to lesser-ranking officials who lacked the incentives and authority to address problems with dispatch and forcefulness. For a Department in desperate need of strong leadership on security issues, this has been a disastrous trend. The bar for future nominees at the upper levels of the Department needs to be raised significantly.

DOE cannot be fixed with a single legislative act: management must follow mandate. The research functions of the labs are vital to the nation's long-term interest, and instituting effective gates between weapons and non-weapons research functions will require disinterested scientific expertise, judicious decision-making, and considerable political finesse. Thus, both Congress and the executive branch—whether along the lines suggested by the Special Investigative Panel or others—should be prepared to monitor the progress of the Department's reforms for years to come. This panel has no illusions about the future of security and counterintelligence at DOE. There is little reason to believe future DOE Secretaries will necessarily share the resolve of Secretary Richardson, or even his interest. When the next Secretary of Energy is sworn in, perhaps in the spring of 2001, the DOE and lab bureaucracies will still have advantages that could give them the upper hand: time and proven skills at artful dodging and passive intransigence.

The Foreign Visitors' and Assignments Program has been and should continue to be a valuable contribution to the scientific and technological progress of the nation. Foreign nationals working under the auspices of US weapons labs have achieved remarkable scientific advances and have contributed immensely to a wide array of America's national security interests, including nonproliferation. Some have made contributions so unique that they are all but irreplaceable. The value of these contacts to the nation should not be lost amid the attempt to address deep, well-founded concerns about security lapses. That said, DOE clearly requires measures to ensure that legitimate use of the research laboratories for scientific collaboration is not an open door to foreign espionage agents. Losing national security secrets should never be accepted as an inevitable cost of obtaining scientific knowledge.

In commenting on security issues at DOE, we believe that both Congressional and Executive Branch leaders have resorted to simplification and hyperbole in the past few months. The panel found neither the dramatic damage assessments nor the categorical reassurances of the Department's advocates to be wholly substantiated. We concur with and encourage many of Secretary Richardson's recent initiatives to address the security problems at the Department, and we are heartened by his aggressive approach and command of the issues. He has recognized the organizational dysfunction and cultural vagaries at DOE and has taken strong, positive steps to try to reverse the legacy of more than 20 years of security mismanagement. However, the Board is extremely skeptical that any reform effort, no matter how well-intentioned, well-designed, and effectively applied, will gain more than a toehold at DOE, given its labyrinthine management structure, fractious and arrogant culture, and the fast-approaching reality of another transition in DOE leadership. Thus, we believe that he has overstated the case when he asserts, as he did several weeks ago, that "Americans can be reassured: our nation's nuclear secrets are, today, safe and secure."

Similarly, the evidence indicating widespread security vulnerabilities at the weapons laboratories has been ignored for far too long, and the work of the Cox Committee and intelligence officials at the Department has been invaluable in gaining the attention of the American public and in helping to focus the political will necessary to resolve these problems. Nonetheless, there have been many attempts to take the valuable coin of damaging new information and decrease its value by manufacturing its counterfeit, innuendo; possible damage has been minted as probable disaster; workaday delay and bureaucratic confusion have been cast as diabolical conspiracies. Enough is enough.

Fundamental change in DOE's institutional culture—including the ingrained attitudes toward security among personnel of the weapons laboratories—will be just as important as organizational redesign. The members of the Special Investigative Panel have never witnessed a bureaucratic culture so thoroughly saturated with cynicism and disregard for authority. Never before has this panel found such a cavalier attitude toward one of the most serious responsibilities in the federal government—control of the design information relating to nuclear weapons. Particularly egregious have been the failures to enforce cyber security measures to protect and control important nuclear weapons design information. Never before has the panel found an agency with the bureaucratic insolence to dispute, delay, and resist implementation of a Presidential directive on security as DOE's bureaucracy tried to do to the Presidential Decision Directive No. 61 in February 1998.

The best nuclear weapons expertise in the US Government resides at the national weapons labs, and the Intelligence Community should better use this asset. For years, the PFIAB has been keen on honing the Intelligence Community's analytic effectiveness on a wide array of nonproliferation areas, including nuclear weapons. We believe that the DOE Office of Intelligence, particularly its analytic component, has historically been an impediment to this goal because of its ineffective attempts to manage the labs' analysis. The office's mission and size (about 70 people) is totally out of step with the Department's intelligence needs. A streamlined intelligence liaison body, much like Department of Treasury's Office of Intelligence Support—which numbers about 20 people, including a 24-hour watch team—would be far more appropriate. It should concentrate on making the Intelligence Community, which has the preponderance of overall analytic experience, more effective in fulfilling the DOE's analysis and collection requirements.

Root Causes

The sources of DOE's difficulties in both overseeing scientific research and maintaining security are numerous and deep. The Special Investigative Panel primarily focused its inquiry on the areas within DOE where the tension between science and security is most critical: the nuclear weapons laboratories.[1] To a lesser extent, the panel examined security issues in other areas of DOE and broad organizational issues that have had a bearing on the functioning of the laboratories.

Inherent in the work of the weapons laboratories, of course, is the basic tension between scientific inquiry, which thrives on freewheeling searches for and wide dissemination of information, and governmental secrecy, which requires just the opposite. But the historical context in which the labs were created and thrived has also figured into their subsequent problems with security.

Big, Byzantine, and Bewildering Bureaucracy

DOE is not one of the federal government's largest agencies in absolute terms, but its organizational structure is widely regarded as one of the most confusing. That structure is another legacy of its origins, and it has made the creation, implementation, coordination, and enforcement of consistent policies very difficult over the years.

The effort to develop the atomic bomb was managed through an unlikely collaboration of the Manhattan Engineering District of the US Army Corps of Engineers (hence the name, "the Manhattan Project") and the University of

California—two vastly dissimilar organizations in both culture and mission. The current form of the Department took shape in the first year of the Carter Administration through the merging of more than 40 different government agencies and organizations, an event from which it has arguably never recovered.

The newly created DOE subsumed the Federal Energy Administration, the Energy Research and Development Administration (ERDA), the Federal Power Commission, and components and programs of several other government agencies. Included were the nuclear weapons research laboratories that were part of the ERDA and, formerly, of the Atomic Energy Commission.

Many of these agencies and organizations have continued to operate under the DOE umbrella with the same organizational structure that they had before joining the Department.

Even before the new Department was created, concerns were raised about how high the nuclear weapons-related operations would rank among the competing priorities of such a large bureaucracy. A study of the issue completed in the last year of the Ford Administration considered three alternatives: shifting the weapons operations to the Department of Defense, creating a new freestanding agency, or keeping the program within ERDA—the options still being discussed more than 20 years later. As one critic of the DOE plan told *The Washington Post*, "Under the AEC, weapons was half the program. Under ERDA, it was one-sixth. Under DOE, it will be one-tenth. It isn't getting the attention it deserves." Although the proportions cited by that critic would prove to be inaccurate, he accurately spotted the direction of the trend.

Lack of Accountability

Depending on the issue at hand, a line worker in a DOE facility might be responsible to DOE headquarters in Washington, a manager in a field office in another state, a private contractor assigned to a DOE project, a research team leader from academia, or a lab director on another floor of the worker's building. For example, prior to Secretary Richardson's restructuring initiative earlier this year, a single laboratory, Sandia, was managed or accountable to nine DOE security organizations.

Last year, after years of reports highlighting the problem of confused lines of authority, DOE was still unable to ensure the effectiveness of security measures because of its inability to hold personnel accountable. A 1998 report lamented that, "short of wholesale contract termination, there did not appear to be adequate penalty/reward systems to ensure effective day-to-day security oversight at the contractor level."[2]

The problem is not only the diffuse nature of authority and accountability in the Department, but it is also the dynamic and often informal character of the authority that does exist. The inherently unpredictable outcomes of major experiments, the fluid missions of research teams, the mobility of individual researchers, the internal competition among laboratories, the ebb and flow of the academic community, the setting and onset of project deadlines, the cyclical nature of the federal budgeting process, and the shifting imperatives of energy and security policies dictated from the White House and Congress all contribute to volatility in the Department's work force and an inability to give the weapons-related functions the priority they deserved. Newcomers, as a result, have an exceedingly hard time when they are assimilated; incumbents have a hard time in trying to administer consistent policies; and outsiders have a hard time divining departmental performance and which leaders and factions are credible. Such problems are not new to government organizations, but DOE's accountability vacuum has only exacerbated them.

Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy direction. As one observer noted in *Science* magazine in 1994, "Every administration sets up a panel to review the national labs. The problem is that nothing is done." The constant managerial turnover over the years has generated

nearly continuous structural reorganizations and repeated security policy reversals. Over the last 12 years, DOE has averaged some kind of major departmental shakeup every two to three years. During that time, security and counterintelligence responsibilities have been "punted" from one office to the next.

Culture and Attitudes

One facet of the culture mentioned more than others is an arrogance borne of the simple fact that nuclear researchers specialize in one of the world's most advanced, challenging, and esoteric fields of knowledge. Nuclear physicists, by definition, are required to think in literally other dimensions not accessible to laymen. Thus it is not surprising that they might bridle under the restraints and regulations of administrators and bureaucrats who do not entirely comprehend the precise nature of the operation being managed.

Operating within a large, complex bureaucracy with transient leaders would tend to only accentuate a scientist's sense of intellectual superiority: if administrators have little more than a vague sense of the contours of a research project, they are likely to have little basis to know which rules and regulations constitute unreasonable burdens on the researchers' activities.

With respect to at least some security issues, the potential for conflicts over priorities is obvious. For example, how are security officials to weigh the risks of unauthorized disclosures during international exchanges if they have only a general familiarity with the cryptic jargon used by the scientists who might participate?

The prevailing culture of the weapons labs is widely perceived as contributing to security and counterintelligence problems. At the very least, restoring public confidence in the ability of the labs to protect nuclear secrets will require a thorough reappraisal of the culture within them.

Changing Times, Changing Missions

The external pressures placed on DOE in general, and the weapons labs in particular, are also worth noting. For more than 50 years, America's nuclear researchers have operated in a maelstrom of shifting and often contradictory attitudes. In the immediate aftermath of World War II, nuclear discoveries were simultaneously hailed as a destructive scourge and a panacea for a wide array of mankind's problems. The production of nuclear arms was regarded during the 1950s and 1960s as one of the best indices of international power and the strength of the nation's military deterrent.

During the 1970s, the nation's leadership turned to nuclear researchers for solutions to the energy crisis at the same time that the general public was becoming more alarmed about the nuclear buildup and the environmental implications of nuclear facilities.

During the past 20 years, some in Congress have repeatedly called for the dissolution of the Department of Energy, which has undoubtedly been a distraction to those trying to make long-term decisions affecting the scope and direction of the research at the labs. And in the aftermath of the Cold War, the Congress has looked to the nation's nuclear weapons labs to help in stabilizing or dismantling nuclear stockpiles in other nations.

Each time that the nation's leadership has made a major change in the Department's priorities or added another mission, it has placed additional pressure on a government agency already struggling to preserve and expand one of its most challenging historical roles: guarantor of the safety, security, and reliability of the nation's nuclear weapons.

Recurring Vulnerabilities

During the past 20 years, six DOE security issues have received the most scrutiny and criticism from both internal and external reviewers: long-term security planning and policy implementation; physical security over facilities and property; screening and monitoring of personnel; protection

of classified and sensitive information, particularly information that is stored electronically in the Department's computers; accounting for nuclear materials; and the foreign visitors' programs.

Management and Planning

Management of security and counterintelligence has suffered from chronic problems since the creation of the Department of Energy in 1977. During the past decade, the mismatch between DOE's security programs and the severity of the threats faced by the Department grew more pronounced. While the number of nations possessing, developing, or seeking weapons of mass destruction continued to rise, America's reliance on foreign scientists and engineers dramatically increased, and warnings mounted about the espionage goals of other nations, and DOE spending on safeguards and security decreased by roughly one-third.[3]

The widening gap between the level of security and the severity of the threat resulted in cases where sensitive nuclear weapons information was certainly lost to espionage. In countless other instances, such information was left vulnerable to theft or duplication for long periods, and the extent to which these serious lapses may have damaged American security is incalculable. DOE's failure to respond to warnings from its own analysts, much less independent sources, underscores the depth of its managerial weakness and inability to implement legitimate policies regarding well-founded threats.

A Sample of Security Issues

Management and Planning

- *Decentralized decisionmaking undermines consistency of policies.*
- *Lack of control of security budget has allowed diversion of funds to other priorities.*
- *Department leaders with little experience in security and intelligence.*
- *Lack of accountability.*

Physical Security

- *Training insufficient for some security personnel.*
- *Nuclear materials stored in aging buildings not designed for containment purposes.*
- *Recurring problems involving lost or stolen property.*
- *Poor management results in unnecessary training and purchasing costs.*

Personnel Security Clearances

- *Extended lags in obtaining clearances, reinvestigating backgrounds, and terminating clearance privileges for former employees.*
- *Some contractors not adequately investigated or subject to drug and substance abuse policies.*
- *Lack of uniform procedures and accurate data.*
- *Inadequate pre-employment screening.*
- *More clearances granted than necessary.*

Protection of Classified Information

- *Poor labeling and tracking of computer media containing classified information.*
- *Problems with lax enforcement of password policies.*
- *Network, e-mail, and Internet connections make transfer of large amounts of data easier.*

Accounting for Nuclear Materials

- *Chronic problems in devising and operating an accurate accounting system of tracking stocks and flows of nuclear materials.*

Foreign Visitors

- *Weak systems for tracking visits and screening backgrounds of visiting scientists.*
- *Decentralization makes monitoring of discussions on sensitive topics difficult.*

During the mid-1980s, the predominant concern of DOE officials was improving the physical security of the nuclear weapons laboratories and plants. Following a January 1983 report[4] that outlined vulnerabilities of the weapons labs to terrorism, the Department embarked on a five-year program of construction and purchases that would see its overall safeguards and security budget roughly double and its spending on upgrades nearly triple. Included was money for additional guards, security training, helicopters, fortified guard towers, vehicle barriers, emergency planning, and advanced alarm systems.[5]

Improving physical security in a wide array of nuclear weapons facilities, whose replacement value was an estimated $100 billion,[6] proved to be difficult. Reports through the late 1980s and early 1990s continued to highlight deficiencies in the management of physical security.

In the late 1980s, priorities began to shift somewhat. Listening devices were discovered in weapons-related facilities,[7] and a 1990 study advised the Department leadership of an intensifying threat from foreign espionage. Less and less able to rely on the former Soviet Union to supply technology and resources, an increasing number of states embarked on campaigns to bridge the economic and technological gap with the United States by developing indigenous capabilities in high-technology areas. The study noted that the freer movement of goods, services, and information in a less hostile world "intensified the prospects and opportunities for espionage as missing pieces of critically needed information became more easily identified."[8]

An intelligence report further highlighted the changing foreign threat to the labs by noting that "new threats are emerging from nontraditional adversaries who target issues key to US national security. DOE facilities and personnel remain priority targets for hostile intelligence collection."[9] Anecdotal evidence corroborates, and intelligence assessments agree, that foreign powers stepped up targeting of DOE during the early 1990s (see the classified Appendix). While this threat may have been taken seriously at the highest levels of the DOE, it was not uniform throughout the Department.

A former FBI senior official noted in discussions with the PFIAB investigative panel that DOE lab scientists during these years appeared naive about the level of sophistication of the nontraditional threat posed by Chinese intelligence collection. The trend in openness to foreign visitors and visits does not indicate any sense of heightened wariness. A 1997 GAO report concluded that, from mid-1988 to the mid-1990s, the number of foreign visitors to key weapons labs increased from 3,800 to 5,900 annually, and sensitive country visitors increased from 500 to more than 1,600. [10] Meanwhile, the DOE budget for counterintelligence was in near-constant decline.

As noted in the previous chapter, federal officials in charge of oversight of nuclear weapons laboratories have historically allowed decision-making on basic aspects of security to be decentralized and diffuse. With their budget spread piecemeal throughout a number of offices, security and counterintelligence officials often found themselves with a weak voice in internal bureaucratic battles and an inability to muster the authority to accomplish its goals. Indeed, an excerpt from a history of the early years of the Atomic Energy Commission reads much like recent studies:

> *Admiral Gingrich, who had just resigned as director of security [in 1949], had expressed to the Joint Committee [on Atomic Energy] a lack of confidence in the Commission's security program. Gingrich complained that decentralization of administrative functions to the field offices had left him with little more than a staff function at headquarters; even there, he said, he did not control all the activities that seemed properly to belong to the director of security*.[11]

More than 30 years later, decentralization still posed a problem for security managers. An internal DOE report in 1990 found that the Department lacked a comprehensive approach to management

of threats and dissemination of information about them.[12] An annual DOE report in 1992 found that security "has suffered from a lack of management focus and inconsistent procedural execution throughout the DOE complex. The result is that personnel are seldom held responsible for their disregard, either intentional or unintentional, of security requirements."[13]

The counterintelligence effort at DOE in the late 1980s and mid-1990s was in its infancy and grossly under-funded stage. Although the Department could have filled its gap in some areas, such as counterintelligence information, through cooperation with the broader Intelligence Community, PFIAB research and interviews indicate that DOE headquarters' relationship with the FBI—the United States' primary domestic CI organization—was strained at best.

In 1998, DOE requested an FBI agent detailee to assist in developing a CI program, but the agent found that DOE failed to provide management support or access to senior DOE decision-makers. A formal relationship with the FBI was apparently not established until 1992: a Memorandum of Understanding between the FBI and DOE on respective responsibilities concerning the coordination and conduct of CI activities in the United States. However, in 1994 two FBI detailees assigned to DOE complained about their limited access and were pulled back to the FBI because of a "lack of control of the CI program by DOE Headquarters, which resulted in futile attempts to better manage the issue of foreign visitors at the laboratories."[14]

The haphazard assortment of agencies and missions folded into DOE has become so confusing as to become a running joke within the institution. In the course of the panel's research and interviews, rare were the senior officials who expressed any sort of confidence in their understanding of the extent of the agency's operations, facilities, or procedures. Time and again, PFIAB panel members posed the elementary questions to senior DOE officials. To whom do you report? To whom are you accountable? The answer, invariably, was, "It depends."

DOE's relationship with the broader Intelligence Community was not well defined until the mid-1990s. Coordination between DOE CI elements and the broader Intelligence Community, according to a 1992 intelligence report, was hampered from the 1980s through the early 1990s by DOE managers' inadequate understanding of the Intelligence Community.[15] The Department did not become a core member of the National Counterintelligence Policy Board (established in 1994 under PDD-24) until 1997.

Over much of the past decade, rather than a heightened sensitivity to espionage threats recognized widely throughout the Intelligence Community, DOE lab officials have operated in an environment that allowed them to be sanguine, if not skeptical. Numerous DOE officials interviewed by the PFIAB panel stated that they believed that the threat perception was weakened further during the administration of Secretary O'Leary, who advanced the labs openness policies and downgraded security as an issue by terminating some security programs instituted by her predecessor.

Even when the CI budget was expanded in the late 1990s, the expenditures fell short of the projected increases. In Fiscal Year 1997, for example, DOE's CI budget was $3.7 million, but the actual expenditures on CI were only two-thirds of that level, $2.3 million. Shortly before the 1997 GAO and FBI reports on DOE's counterintelligence posture were issued, DOE began instituting changes to beef up its counterintelligence and foreign intelligence analytic capabilities.[16]

When DOE did devote its considerable resources to security, it too often faltered in implementation. A report sent to the Secretary in January 1994 noted "growing confusion within the Department with respect to Headquarters' guidance for safeguards and security. At this time, there is no single office at Headquarters responsible for the safeguards and security program. Most recently, a number

of program offices have substantially expanded their safeguards and security staff to office-size organizations. These multiple safeguards and security offices have resulted in duplication of guidance, unnecessary requests for information and clarification, and inefficient program execution. Unchecked, this counterproductive tendency threatens the success of the overall safeguards and security effort."[17]

A 1996 DOE Inspector General report found that security personnel at the weapons programs had purchased and stockpiled far more firepower—ranging from handguns and rifles to submachine guns and grenade launchers—than could ever be used in an actual emergency. The Oak Ridge facilities had more than three weapons per armed security officer—on and off duty; Los Alamos National Laboratory had more than four.[18]

Around the same time, GAO security audits of the research laboratories at these sites found lax procedures for issuing access passes to secure areas, inadequate prescreening of the more than 1,500 visitors from sensitive countries that visited the weapons laboratories annually, and poor tracking of the content of discussions with foreign visitors. The implication: foreign agents could probably not shoot their way past the concertina wires and bolted doors to seize secrets from US weapons laboratories, but they would not need to do so. They could probably apply for an access pass, walk in the front door, and strike up a conversation.

Physical Security

The physical security of the Department of Energy's weapons-related programs is roughly divided into two essential functions: tracking and control over the property and equipment within the weapons-related laboratories and keeping unwarranted intruders out, often referred to as the realm of "guns, guards, and gates."

The general approach to security, of course, was defined by the emphasis on secrecy associated with nuclear weapons program during World War II. Los Alamos National Laboratory was created as a "closed city"—a community with a high degree of self-sufficiency, clearly defined and protected boundaries, and a minimum of ingress from and egress to the outer world. Although the community is no longer "closed," the weapons laboratories at Los Alamos, like those at the other national laboratories, still retain formidable physical protections and barriers. In examining the history of the laboratories, the panel found only a few instances where an outsider could successfully penetrate the grounds of an operation by destruction of a physical safeguard or direct violent assault.

In visits to several of the weapons laboratories, the members of the Special Investigative Panel were impressed by the great amount of attention and investment devoted to perimeter control, weaponry, and security of building entrances and exits. Indeed, one cannot help but be struck by the forbidding and formidable garrison-type atmosphere that is prevalent at many of the facilities: barbed wire, chain-link fences, electronic sensors, and surveillance cameras. Further, the panel recognizes that the labs themselves have developed and produced some of the most sophisticated technical security devices in the world. Nonetheless, DOE reports and external reviews since at least 1984 have continued to raise concerns about aging security systems.[19]

Management of the secure environments at the laboratories has posed more serious problems. As noted earlier, DOE may be spending too much money in some areas, buying more weapons than could conceivably be used in an emergency situation. In other cases, it may be spending too little. Budget cuts in the early and mid-1990s led to 40- to 50-percent declines in officer strength and over-reliance on local law enforcement. Resources became so low that normal protective force operations required "the use of overtime scheduling to accomplish routine site protection."[20] GAO has found an assortment of problems at Los Alamos over the past decade: security personnel failed basic tests in such tasks as firing weapons, using a baton, or handcuffing a suspect and inaccurate and

incomplete records were kept on security training.[21] Other DOE facilities have had substantial problems in management of physical property:

- In 1990, Lawrence Livermore Laboratory could not account for 16 percent of its inventory of government equipment, acquired at a cost of $18.6 million.[22]
- In 1993, DOE sold 57 components of nuclear reprocessing equipment and associated documents, including blueprints, to an Idaho salvage dealer. Much of what was sold was subsequently found to be potentially useful to any nation attempting to develop or advance its own reprocessing operation.[23]
- Following a GAO report in 1994, which found that the Rocky Flats facility was unable to account for large pieces of equipment such as forklifts and a semi-trailer, some $21 million in inventory was written off.[24]

DOE had begun to consolidate its growing stockpile of sensitive nuclear material by 1992, but a 1997 DOE report to the Secretary found that significant quantities of the material "remain in aging buildings and structures, ranging in age from 12 to 50 years that were never intended for use as storage facilities for extended periods."[25]

Screening and Monitoring of Personnel

Insider threats to security have been a chronic problem at the nation's weapons laboratories. From the earliest years, the importance of the labs' missions and their decentralized structure have had an uneasy coexistence with the need for thorough background investigations of researchers and personnel needing access to sensitive areas and information.

In 1947, the incoming director of security for the AEC was greeted with a backlog of more than 13,000 background investigations and a process where clearances had been dispersed to field offices that operated with few formal guidelines.[26]

Forty years later, GAO found that the backlog of personnel security investigations had increased more than nine-fold, to more than 120,000. Moreover, many clearances recorded as valid in the Department's records should have been terminated years before.[27]

Even after DOE discovered listening devices in some of its weapons laboratories, security audits found that thousands of "Q" clearances were being given to inappropriate personnel.[28]

The research of the PFIAB panel found that problems with personnel security clearances, while mitigated in some aspects, have persisted to an alarming degree. From the mid-1980s through the mid-1990s, the DOE Inspector General repeatedly warned Department officials that personnel were receiving clearances that were much higher than warranted and that outdated clearances were not being withdrawn on a timely basis. The issue became more urgent with the discovery of a clandestine surveillance device at a nuclear facility.[29]

DOE Inspector General reports in 1990 and 1991 found that one of the weapons laboratories had granted "Q" clearances (which provide access to US Government nuclear weapons data) to more than 2,000 employees who did not need access to classified information.[30] A 1992 report to the Secretary of Energy noted that "DOE grants clearances requested by its three major defense program sponsored labs based on lab policies to clear all employees regardless of whether actual access to classified interests is required for job performance."[31]

Three years later, a review of personnel security informed the Secretary that there were "individuals who held security clearances for convenience only and limited security clearances to those individuals requiring direct access to classified matter or [special nuclear materials] to perform official duties."[32]

More recent evidence is no more reassuring. A counterintelligence investigation at a nuclear facility discovered that the subject of an inquiry had been granted a "Q" clearance simply to avoid

the delay caused by the normal processing of a visit.[33] During that same year, an illegal telephone wiretap was discovered at the same lab. The employee who installed it confessed but was not prosecuted by the government.[34]

Protection of Classified and Sensitive Information

Two vulnerabilities regarding classified and sensitive information at DOE have recurred repeatedly throughout the past 20 years: inappropriate release of classified information, either directly through inadvertence or indirectly through improper declassification; and the increasing mobility of classified and sensitive information through electronic media, such as computers.

As computers have progressed from large mainframes of the 1950s and 1960s to desktop models in the 1980s and decentralized networks in the 1990s, it has become progressively easier for individuals to retrieve and transport large amounts of data from one location to another. This has presented an obvious problem for secure environments. GAO found in 1991 that DOE inspections revealed more than 220 security weaknesses in computer systems across 16 facilities. Examples included a lack of management plans, inadequate access controls, and failures to test for compliance with security procedures.[35]

As a 1996 DOE report to the President said, "adversaries no longer have to scale a fence, defeat sensors, or bypass armed guards to steal nuclear or leading-edge 'know-how' or to shut down our critical infrastructure. They merely have to defeat the less ominous obstacles of cyber-defense."[36]

Computer systems at some DOE facilities were so easy to access that even Department analysts likened them to "automatic teller machines, [allowing] unauthorized withdrawals at our nation's expense."

DOE's cyber defenses were, in fact, found to be "less ominous obstacles." In 1994, an internal DOE review found that despite security improvement "users of unclassified computers continue to compromise classified information due to ongoing inadequacies in user awareness training, adherence to procedures, enforcement of security policies, and DOE and [lab] line management oversight."[37] Also in 1994, a report to the Energy Secretary cited five areas of concern: "failure to properly accredit systems processing classified information, lack of controls to provide access authorities and proper password management; no configuration management; improper labeling of magnetic media; and failure to perform management reviews."[38]

Apparently, the warnings were to no avail. A year later, the annual report to the Secretary noted, "Overall, findings and surveys, much like last year, continue to reflect deficiencies in self-inspections and procedural requirements or inappropriate or inadequate site guidance … In the area of classified matter protection and control, like last year, marking, accountability, protection, and storage deficiencies are most numerous."[39]

Some reports made extra efforts to puncture through the fog of bureaucratic language. A 1995 report to the President noted, "By placing sensitive information on information systems, we increase the likelihood that inimitable interests, external and internal, will treat those systems as virtual automatic teller machines, making unauthorized withdrawals at our nation's expenses." Indeed, a report found security breaches at one of the major weapons facility in which documents with unclassified but sensitive information "were found to be stored on systems that were readily accessible to anyone with Internet access."[40] In other instances, personnel were found to be sending classified information to outsiders via an unclassified e-mail system.[41]

In 1986, the DOE Office of Safeguards and Quality Assessment issued an inspection report on a weapons lab that warned of shortcomings in computer security and noted that the "ability of

[a] user to deliberately declassify a classified file without detection and move classified information from the secure partition to the open partition can be made available to any authorized user either on or off site."[42] The warning turned out to be on the mark. In April 2001, Energy Secretary Bill Richardson issued the statement, "While I cannot comment on the specifics, I can confirm that classified nuclear weapons computer codes at Los Alamos were transferred to an unclassified computer system. This kind of egregious security breach is absolutely unacceptable."

Even though the hard evidence points to only sporadic penetrations of the labs by foreign intelligence services, volumes of sensitive and classified information may have been lost over the years—via discarded or purloined documents, uninformed and often improperly vetted employees, and a maze of uncontrolled computer links. In one recent case discovered by PFIAB, lab officials initially refused to rectify a security vulnerability because "no probability is assigned to [a loss of sensitive information], just the allegation that it is possible."[43]

As recent as last year's annual DOE report to the President, security analysts were finding "numerous incidents of classified information being placed on unclassified systems, including several since the development of a corrective action plan in July 1998."[44]

Foreign Visitors and Assignments Program

True to the tradition of international partnership molded by the experiences of the Manhattan Project, the weapons labs have remained a reservoir of the best international scientific talent. Recent examples abound: a supercomputing team from Oak Ridge National Lab, made up of three PRC citizens and a Hungarian, recently won the Gordon Bell Prize; a Bulgarian and a Canadian, both world-class scientists, are helping Lawrence Livermore National Lab solve problems in fluid dynamics; a Spanish scientist, also at Livermore, is collaborating with colleagues on laser propagation.

For more than a decade, the increasing prominence of foreign visitors in the weapons labs has increased concern about security risks. The PFIAB found that, as early as 1985, the DCI raised concerns with the Energy Secretary about the foreign visitors' program. A year later, researchers conducting internal DOE review could find only scant data on the number and composition of foreign nationals at the weapons labs. Although intelligence officials drafted suggestions for DOE's foreign visitor control program, PFIAB found little evidence of reform efforts until the tenure of Secretary Watkins.

A 1988 GAO report cited DOE for failing "to obtain timely and adequate information on foreign visitors before allowing them access to the laboratories." The GAO found three cases where DOE allowed visitors with questionable backgrounds—possible foreign agents—access to the labs. In addition, the GAO found that about 10 percent of 637 visitors from sensitive countries were associated with foreign organizations suspected of conducting nuclear weapons activities, but DOE did not request background data on them prior to their visit. DOE also had not conducted its own review of the visit and assignment program at the weapons labs despite the DOE requirement to conduct audits or reviews at a minimum of every five years. Moreover, GAO reported that few post-visit or host reports required by DOE Order 12402 were submitted within 30 days of the visitors' departure, and some were never completed.[45]

In 1989, DOE revised its foreign visitor policy and commissioned an external study on the extent and significance of the foreign visitor problem. DOE's effort to track and vet visitors, however, still lagged the expansion of the visitor program, allowing foreigners with suspicious backgrounds to gain access to weapons facilities. A study published in June 1990 indicated DOE had a "crippling lack of essential data, most notably no centralized, retrievable listing of foreign national visitors to government facilities."[46]

By September 1992, DOE had instituted Visitor Assignment Management System (VAMS)

databases to track visitors and assignees requesting to visit DOE. The system, however, failed to provide links between the labs that could be used for CI analysis and crosschecking of prospective visitors. Moreover, labs frequently did not even use the database and failed to enter visitor information. Instead, each lab independently developed its own computer program.

Reviews of security determined that, despite an increase of more than 50 percent in foreign visits to the labs from the mid-1980s to the mid-1990s, DOE controls on foreign visitors actually weakened in two critical areas: screening for visitors that may pose security risks and monitoring the content of discussions that might disclose classified information.

In 1994, DOE headquarters delegated greater authority to approve non-sensitive country visitors to the laboratories, approving a partial exception for Los Alamos and Sandia National Laboratories to forego background checks to help "reduce costs and processing backlogs." This resulted in almost automatic approval of some foreign visitors and fewer background checks. The FBI and GAO subsequently found that "questionable visitors, including suspected foreign intelligence agents, had access to the laboratories without DOE and/or laboratory officials' advance knowledge of the visitors' backgrounds."[47]

Changes in records checks over the past decade also made it easier for individuals from sensitive countries to gain access to the laboratories. In 1988, for example, all visitors from Communist countries required records checks regardless of the purpose of the visit. By 1996, records checks were required for visitors from only sensitive countries who visited secure areas or discussed sensitive subjects.

In 1996 an internal DOE task force determined that the Department's definitions of sensitive topics were not specific enough to be useful. The task force directed the DOE office of intelligence to develop a new methodology for defining sensitive topics, but did not set a due date. The 1996 group also called for a Deputy Secretary–level review of foreign visits and assignments to be completed by June 1997. [48] The PFIAB panel found no evidence to suggest that these tasks were accomplished.

In 1997, GAO found that DOE lacked clear criteria for identifying visits that involve sensitive subjects; US scientists may have discussed sensitive subjects with foreign nationals without DOE's knowledge or approval; and the Department's counterintelligence program had failed to produce comprehensive threat assessments that would identify likely facilities, technologies, and programs targeted by foreign intelligence.[49] The study found that record checks were still not regularly conducted on foreign visitors from sensitive countries.[50] Last year, 7,600 foreign scientists visited the weapons labs.[51] Of that total, about 34 percent were from countries that are designated "sensitive" by the Department of Energy—meaning they represent a hostile intelligence threat. The GAO reported last year that foreign nationals had been allowed after-hours and unescorted access to buildings.[52]

Responsibility

While cultural, structural, and historical problems have all figured into the management and security and counterintelligence failures of DOE, they should not be construed as an excuse for the deplorable irresponsibility within the agency, the pattern of inaction from those charged with implementation of policies, or the inconsistency of those in leadership positions. The panel identified numerous instances in which individuals were presented with glaring problems yet responded with foot-dragging, finger-pointing, bland reassurances, obfuscation, and even misrepresentations.

The record of inattention and "false start" reforms goes back to the beginning of DOE. There have been several Presidents; National Security Advisors; Energy Secretaries, Deputy Secretaries, Assistant Secretaries, and Lab Directors; DOE Office Directors and Lab managers; and Energy Department bureaucrats and Lab scientists who all must shoulder the responsibility and accountability.

As noted above, severe lapses in the security of the nation's most critical technology, data, and materials were manifest at the creation of the DOE more than 20 years ago. Many, if not most, of the problems were identified repeatedly. Still, reforms flagged amid a lack of discipline and accountability. The fact that virtually every one of those problems persisted—indeed, many of the problems still exist—indicates a lack of sufficient attention by every President, Energy Secretary, and Congress.

This determination is in no way a capitulation to the standard of "everyone is responsible, therefore no one is responsible." Quite the contrary, even a casual reading of the open-source reports on the Department's problems presents one with a compelling narrative of incompetence that should have merited the aggressive action of the nation's leadership. Few transgressions could violate the national trust more than inattention to one's direct responsibility for controlling the technology of weapons of mass destruction.

The PFIAB was not empowered, nor was it charged, to make determinations of whether specific acts of espionage or malfeasance occurred regarding alleged security lapses at the weapons labs. The PFIAB also was not tasked to issue performance appraisals of the various Presidents, Energy Secretaries, or members of the Congressional leadership during their respective terms in office. However, an inquiry into the extent to which the system of administrative accountability and responsibility broke down at various times in history has been necessary to fulfill our charter. In fairness, we have tried to examine the nature of the security problems at DOE's weapons labs in many respects and at many levels, ranging from the circumstances of individuals and the dynamics of group behavior to the effectiveness of mid–level management, the clarity of the laws and regulations affecting the Department, and the effectiveness of leadership initiatives.

The Record of the Clinton Team

To its credit, in the past two years the Clinton Administration has proposed and begun to implement some of the most far-reaching reforms in DOE's history. The 1998 Presidential Decision Directive on DOE counterintelligence (PDD-61) and Secretary Richardson's initiatives are both substantial and positive steps.

However, the speed and sweep of the Administration's ongoing response does not absolve it of its responsibility in years past. At the outset of the Clinton Administration—in 1993, when it inherited responsibility for DOE and the glaring record of mismanagement of the weapons laboratories—the incoming leadership did not give the security and counterintelligence problems at the labs the priority and attention they warranted. It will be incumbent on the DOE transition team for the incoming administration in 2001 to pay particular heed to these issues.

While the track record of previous administrations' responses to DOE's problems is mixed, the panel members believe that the gravity of the security and counterintelligence mismanagement at the Department will, and should, overshadow post facto claims of due diligence by any administration—including the current one. Asserting that the degree of failure or success with DOE from one administration to the next is relative is, one might say, gilding a fig leaf.

Each successive administration had more evidence of DOE's systemic failures in hand: the Reagan Administration arrived to find several years' worth of troubling evidence from the Carter, Ford, and Nixon years; the evidence had mounted higher by the time the Bush Administration took over; and even higher when the Clinton Administration came in. The Clinton Administration has acted forcefully, but it took pressure from below and outside the Administration to get the attention of

the leadership, and there is some evidence to raise questions about whether its actions came later than they should have, given the course of events that led the recent flurry of activity.

The 1995 "Walk-In" Document

In 1995, a US intelligence agency obtained information that has come to be called the "walk-in" document. This document is a classified PRC report that contains a discussion of various US nuclear warheads. The PFIAB has carefully reviewed this document, related information, and the circumstances surrounding its delivery. Serious questions remain as to when it was written, why it was written, and why it was provided to the United States. We need not resolve these questions. The document unquestionably contains some information that is still highly sensitive, including descriptions, in varying degrees of specificity, of technical characteristics of seven US thermonuclear warheads. This information had been widely available within the US nuclear weapons community, including the weapons labs, other parts of DOE, the Department of Defense, and private contractors, for more than a decade. For example, key technical information concerning the W-88 warhead had been available to numerous US Government and military entities since at least 1983 and could well have come from many organizations other than the weapons labs.

W-88 Investigation

Despite the disclosure of information concerning seven warheads, despite the potential that the source or sources of these disclosures were other than the bomb designers at the national weapons labs, and despite the potential that the disclosures occurred as early as 1982, only one investigation was initiated. That investigation focused on only one warhead—the W-88—only one category of potential sources—bomb designers at the national labs—and only a four-year window of opportunity. It should have been pursued in a more comprehensive manner. The allegations raised in the investigation should still be pursued vigorously, and the inquiry should be fully explored regardless of the conclusions that may result.

The episode began as an administrative inquiry conducted by the DOE Office of Energy Intelligence, with limited assistance from the FBI. It developed into an FBI investigation, which is still under way today. Allegations concerning this case and related activities highlighted the need for improvements in the DOE's counterintelligence program, led along the way to the issuance of a Presidential Decision Directive revamping the DOE's counterintelligence program, formed a substantial part of the information underlying the Cox Committee's conclusions on nuclear weapons information, and ultimately led, at least in part, to the President's decision to ask this Board to evaluate security and counterintelligence at the DOE's weapons labs.

It is not within the mandate of our review to solve the W-88 case or any other potential compromises of nuclear weapons information. Further, it is not within our mandate to conduct a comprehensive and conclusive evaluation of the handling of the W-88 investigation by the Department of Justice and FBI.

It is, however, explicitly within our mandate to identify additional steps that may need to be taken to address the security and counterintelligence threats to the weapons labs. Also, it is within our standing PFIAB obligation under Executive Order 12863 to assess the adequacy of counterintelligence activities beyond the labs. In this regard, what we have learned from our limited review of the W-88 case and other cases are significant lessons that extend well beyond these particular cases. These lessons relate directly to additional steps we believe must be taken to strengthen our safeguards against current security and foreign intelligence threats.

We have learned, for example, that under the current personnel security clearance system a person who is under FBI investigation for suspected counterintelligence activities may sometimes be granted a new or renewed clearance.

We also have learned that, although the written standards for granting a first clearance and for renewing an existing clearance may be identical, the actual practice that has developed—certainly within DOE and we strongly suspect elsewhere—is that clearance renewals will be granted on a lower standard. We find such inconsistency unacceptable. We think it appropriate for the National Security Council to review and resolve these issues.

We have also learned that the legal weapons designed to fight the counterintelligence battles of the 1970s have not necessarily been rigorously adapted to fight the counterintelligence battles of the 1990s (and beyond). For example, with the passage of more than 20 years since the enactment of the Foreign Intelligence Surveillance Act (FISA) of 1978, it may no longer be adequate to address the counterintelligence threats of the new millennium. We take no position on whether the statute itself needs to be changed. It may well still be sufficient. However, based on all of the information we have reviewed and the interviews we have conducted and without expressing a view as to the appropriateness of the DOJ decision in the W-88 case, we do believe that the DOJ may be applying the FISA in a manner that is too restrictive, particularly in light of the evolution of a very sophisticated counterintelligence threat and the ongoing revolution in information systems. We also are concerned by the lack of uniform application across the government of various other investigative tools, such as employee waivers that grant officials appropriate authority to monitor sensitive government computer systems.

Moreover, there does not exist today a systematic process to ensure that the competing interests of law enforcement and national security are appropriately balanced. Law enforcement, rightly so, is committed to building prosecutable cases. Leaving an espionage suspect in place to facilitate the gathering of more evidence often furthers this goal. The national security interest, in contrast, is often furthered by immediately removing a suspect from access to sensitive information to avoid additional compromises. Striking the proper balance is never easy. It is made all the more difficult when there is no regular process to ensure that balance is struck. We have learned in our review that this difficult decision often is made by officials who either are too focused on the investigative details or are too unaware of the details to make a balanced decision. This is another matter deserving National Security Council attention.

PFIAB Evaluation of the Intelligence Community Damage Assessment

Following receipt of the "walk-in" document, CIA, DOE, Congress, and others conducted numerous analyses in an effort to determine the extent of the classified nuclear weapons information the PRC has acquired and the resultant threat to US national security. Opinions expressed in the media and elsewhere have ranged from one extreme to the other. On one end of the spectrum is the view that the Chinese have acquired very little classified information and can do little with it. On the other end is the view that the Chinese have nearly duplicated the W-88 warhead.

After reviewing the available intelligence and interviewing the major participants in many of these studies, we conclude that none of these extreme views holds water. For us, the most accurate assessment of China's acquisition of classified US nuclear weapons information and the resultant threat to US national security is presented in the April 1999 Intelligence Community Damage Assessment. Written by a team of experts, this assessment was reviewed and endorsed by an independent panel of national security and nuclear weapons specialists, chaired by Admiral David Jeremiah. We substantially agree with the assessment's analysis and endorse its key findings.

Presidential Decision Directive 61: Birth and Intent

In mid-1997, it became clear to an increasingly broader range of senior administration officials that DOE's counterintelligence program was in serious trouble.[53] In late July 1997, DOE officials briefed the President's National Security

Advisor, who concluded that, while the real magnitude and national security implications of the suspected espionage needed closer scrutiny, there was, nonetheless, a solid basis for taking steps to strengthen counterintelligence measures at the labs. He requested an independent CIA assessment of China's nuclear program and the impact of US nuclear information, and he directed that the National Counterintelligence Policy Board (NACIPB)[54] review the DOE counterintelligence program. In September 1997, the National Security Advisor received the CIA assessment, and the NACIPB reported back that it had found "systemic and serious CI and security problems at DOE [had] been well documented over at least a ten year period" and "few of the recommendations in the past studies [had] been implemented." The NACIPB made 25 recommendations to significantly restructure the DOE CI program; it also proposed that a Presidential Decision Directive or Executive Order be handed down to effect these changes.

At a meeting on 15 October, the Director of Central Intelligence (DCI) and the FBI Director discussed with Secretary Pena and his Deputy Secretary the need to reform the DOE CI program. The DCI and FBI Director sought to make clear that there was an urgent need to act immediately, and "despite all the studies conducted, experience over time [had] shown that DOE's structure and culture make reform difficult, if not impossible, from within." All agreed to develop an action plan that would serve as the basis for a Presidential Decision Directive (PDD). Several senior officials involved felt that the necessary reforms would—without the mandate of a Presidential directive—have little hope of overcoming the anticipated bureaucratic resistance, both at DOE headquarters and at the labs. There was a clear fear that, "if the Secretary spoke, the bureaucracy wouldn't listen; if the President spoke, the bureaucracy might at least listen."

During the winter of 1997, the NSC coordinated a draft PDD among the many agencies and departments involved. Serious disagreements arose over several issues, particularly the creation of independent reporting lines to the Secretary for the Intelligence and Counterintelligence Offices. Also at issue was the subordination of the CI officers at the labs. Much of the resistance stemmed simply from individuals interested in preserving their turf won in previous DOE bureaucratic battles. After much bureaucratic maneuvering and even vicious infighting, these issues were finally resolved, or so it seemed; and on 11 February 1998, the President signed and issued the directive as PDD-61.

The full PDD remains classified. In our view, among the most significant of the 13 initiatives directed by PDD-61 are:

- The CI and foreign intelligence (FI) elements would be reconfigured into two independent offices and report directly to the Secretary of Energy.
- The Director of the new Office of CI (OCI) would be a senior executive from the FBI and would have direct access to the Secretary of Energy, the DCI, and the Director of the FBI.
- Existing DOE contracts with the labs would be amended to include CI program goals and objectives and performance measures to evaluate compliance with these contractual obligations, and CI personnel assigned to the labs would have direct access to the lab directors and would concurrently report to the Director OCI.
- Ninety days after his arrival, the incoming Director OCI would prepare a report for the Secretary of Energy that would address progress on the initiative, a strategic plan for achieving long-term goals, and recommendations on whether and to what extent other organizational changes may be necessary to strengthen CI.
- Within 120 days, the Secretary of Energy would advise the Assistant to the President for National Security Affairs on the actions taken and specific remedies designed to implement this directive.

On 1 April 1998, a senior executive from the FBI assumed his duties as the Director of the OCI and began his 90-day study. He completed and forwarded the study to the Secretary of Energy on 1 July, the day after Secretary Pena resigned. The Acting Secretary, Elizabeth A. Moler, led a

review of the study and its recommendations. On 18 August, Secretary Richardson was sworn in. On 13 November, Richardson submitted the CI Action Plan required by the PDD to the National Security Advisor. He also met with lab CI Directors and DOE headquarters CI and Intelligence staff to discuss the implementation plan. The implementation plan continued to be developed by his staff, and the completed plan was delivered to Secretary Richardson on 3 February 1999. It was issued to the labs on 4 March.

Timeliness of PDD-61

Criticism has been raised that the PDD took too long to issue and has taken too long to implement. Although the current National Security Advisor was briefed on counterintelligence concerns by DOE officials in April 1996, we are not convinced that the briefing provided a sufficient basis to require initiation of a broad Presidential directive at that time. We are convinced, however, that the July 1997 briefing, which we are persuaded was much more comprehensive, was sufficient to warrant aggressive White House action. We believe that, while the resulting PDD was developed and issued within a customary amount of time, these issues had such national security gravity that it should have been handled with more dispatch. It is not surprising that there were disagreements over various issues. It is very disturbing that the DOE bureaucracy dug in its heels so deeply in resisting clearly needed reform. In fact, we believe that the NACIPB, created by PDD in 1994, was a critical factor in ram-rodding the PDD through to signature. Before 1994, there was no real structure or effective process for handling these kinds of issues in a methodical way. Had the new structure not been in place and working, we doubt if the PDD would have made it.

With regard to timeliness of implementation, we have far greater concern. The PFIAB recognized that senior DOE officials would require some time to evaluate the new OCI Director's 90-day study and that Secretary Richardson did not assume his DOE duties until mid-August, but we find unacceptable the more than four months that elapsed before DOE advised the National Security Advisor on the actions taken and specific remedies developed to implement the Presidential directive, particularly one so crucial.

More critically, we are disturbed by bureaucratic foot-dragging and even recalcitrance that ensued after issuance of the Presidential Decision Directive. Severe disagreements erupted over several issues, including whether the CI program would apply to all of the labs, and not just the weapons labs and the extent to which polygraph examinations would be used in the personnel security program. We understand that some DOE officials declined to assist in the implementation simply by declaring that, "It won't work." The polygraph program was finally accepted into the DOE's security reforms only after the National Security Advisor and the DCI personally interceded. The fact that the Secretary's implementation plan was not issued to the labs until more than a year after the PDD was issued tells us DOE is still unconvinced of Presidential authority. We find worrisome the reports of repeated and recent resistance by Office of Management and Budget (OMB) officials toward requests for funding to implement the counterintelligence reforms mandated by PDD-61. We find vexing the reports we heard of OMB budgeters lecturing other government officials on the "unimportance" of counterintelligence at DOE.

Secretary Richardson's Initiatives

Since November 1998 and especially since April of this year, Secretary Richardson has taken commendable steps to address DOE's security and counterintelligence deficiencies. In November 2000, in the action plan required by PDD-61, Secretary Richardson detailed 31 actions to be taken to reform DOE's counterintelligence program. These actions addressed the structure of the counterintelligence program, selection and training of field counterintelligence personnel, counterintelligence analysis, counterintelligence and security awareness, protections against potential "insider threats," computer security, and

relationships with the FBI, the Central Intelligence Agency, and the National Security Agency.

Though many matters addressed in the action plan would require further evaluation before specific actions would be taken, immediate steps included granting to the OCI direct responsibility for programming and funding counterintelligence activities of all DOE field offices and laboratories, granting the Director OCI the sole authority to propose candidates to serve as the counterintelligence officers at the weapons labs, and instituting a policy for a polygraph program for employees with access to sensitive information.

In April 1999, in an effort to eliminate multiple reporting channels and to improve lines of communications, direction, and accountability, Secretary Richardson ordered changes in the Department's management structure. In short, each of the 11 field offices reports to a Lead Program Secretarial Office (LPSO). The LPSO has "overall line accountability for site-wide environment, safety and health, for safeguards and security and for the implementation of policy promulgated by headquarters staff and support functions." A newly established Field Management Council is to be charged with program integration.

In May 1999, Secretary Richardson announced substantial restructuring of the security apparatus at DOE. Among these is the new Office of Security and Emergency Operations, which will report directly to the Secretary. It consists of the Office of the Chief Information Officer, the Office of Emergency Management and Response, and the Office of Security Affairs, which will include the Office of Safeguards and Security, the Office of Nuclear and National Security Information, the Office of Foreign Visits and Assignments, and the Office of Plutonium, Uranium, and Special Material Inventory. This office is responsible for all safeguards and security policy, cybersecurity, and emergency functions throughout DOE.

Also announced was the creation of the Office of Independent Oversight and Performance Assurance. It also will report directly to the Secretary to provide independent oversight for safeguards and security, special nuclear materials accountability, and other related areas.

To support additional cyber-security improvements, DOE will be asking Congress for an additional $50 million over the next two years. Improvements are to include continual monitoring of DOE computers for unauthorized and improper use. Also, new controls will be placed on computers and workstations, removable media, removable drives, and other devices that could be used to download files. In addition, warning "banners" are now mandatory on all computer systems to alert users that these systems are subject to search and review at the government's discretion. Cybersecurity training is also to be improved.

Secretary Richardson further announced additional measures designed to strengthen DOE's counterintelligence program. They include a requirement that DOE officials responsible for maintaining personnel security clearances be notified of any information that might affect the issuance or maintenance of such a clearance, even when the information does not rise to the level of a criminal charge; and mandatory reporting by all DOE employees of any substantive contact with foreign nationals from sensitive countries. DOE also plans to strengthen its Security Management Board; accelerate actions necessary to correct deficiencies in security identified in the 1997/1998 Annual Report to the President on Safeguards and Security; expedite improvements in the physical security of DOE nuclear weapons sites; and delay the automatic declassification of documents more than 25 years old.

In sum, as of mid-June 1999, progress has been made in addressing counterintelligence and security. Of note, all of the PDD-61 requirements are reported to have been substantially implemented. Other important steps also reportedly have been completed. Among these are the assignment of experienced counterintelligence officers to the weapons labs.

Prospects for Reforms

Although we applaud Secretary Richardson's initiative, we seriously doubt that his initiatives will achieve lasting success. Though certainly significant steps in the right direction, Secretary Richardson's initiatives have not yet solved the many problems. Significant objectives, all of which were identified in the DOE OCI study completed nearly a year ago, have not yet been fully achieved. Among these unmet objectives are revising the DOE policy on foreign visits and establishing an effective polygraph examination program for selected, high-risk programs. Moreover, the Richardson initiatives simply do not go far enough.

These moves have not yet accomplished some of the smallest fixes despite huge levels of attention and Secretarial priority. Consider the following example: with all the emphasis of late on computer security, including a weeks-long standdown of the weapons labs computer systems directed by the Secretary, the stark fact remains that, as of the date of this report, a nefarious employee can still download secret nuclear weapons information to a tape, put it in his or her pocket, and walk out the door. Money cannot really be the issue. The annual DOE budget is already $18 billion. There must be some other reason.

Under the Richardson plan, even if the new "Security Czar" is given complete authority over the more than $800 million ostensibly allocated each year to security of nuclear weapons-related functions in DOE, he will still have to cross borders into other people's fiefdoms, causing certain turmoil and infighting. If he gets no direct budget authority, he will be left with little more than policy guidance. Even then, as the head of a staff office under the most recent Secretary Richardson reorganization, he has to get the approval of yet another fiefdom, the newly created Field Management Council, before he can issue policy guidance. Moreover, he is unlikely to have much success in obtaining approval from that body when he is not even a member, and the majority of those who are members are the very program managers that his policy guidance would affect.

Trouble Ahead

Perhaps the most troubling aspect of the PFIAB's inquiry is the evidence that the lab bureaucracies—after months at the epicenter of an espionage scandal with serious implications for US foreign policy—are still resisting reforms. Equally disconcerting, other agencies have joined the security skeptics' list. In the past few weeks, officials from DOE and other agencies have reported to the Rudman panel:

- There is a heightened attention to security at the most senior levels of DOE and the labs, but at the midlevel tiers of management there has been lackluster response and "business as usual."
- Unclassified but sensitive computer networks at several weapons labs are still riddled with vulnerabilities.
- Buildings that do not meet DOE security standards are still being used for open storage of weapons parts.
- Foreign nationals—some from sensitive countries—residing outside a weapons lab have remote dial-up access to unclassified networks without any monitoring by the lab.
- In an area of a weapons lab frequented by foreign nationals, a safe containing restricted data was found unsecured. Guards had not checked the safe since August 1998. When confronted with the violation, a midlevel official is said to have implied that it was not an actual security lapse because the lock had to be "jiggled" to open the safe door.
- A weapons lab was instructed to monitor its outgoing e-mail for possible security lapses. The lab took the minimal action necessary; it began monitoring e-mails but did not monitor the files attached to e-mails.
- When Secretary Richardson ordered the recent computer stand down, there was great resistance, and when it came time to decide if the labs' computers could be turned on again, a bevy of DOE officials fought to have final approval power.

Security and Counterintelligence Accountability

The agency director should issue clear guidelines on security accountability. The agency security chief must be accountable to the agency director for security policy at the labs, and the lab directors must be accountable to the agency director for compliance. The same system and process should be established to instill accountability among counterintelligence officials.

Attentive, independent oversight will be critical to ensuring high standards of security and counterintelligence performance at the new agency. In that regard, we welcome Senator John Warner's recent legislative initiative to create a small, dedicated panel to oversee security and counterintelligence performance at the weapons labs. This oversight should include an annual certification process.

Personnel Security

An Effective Personnel Security Program. The agency director should immediately undertake a total revamping of the "Q" clearance program and look to the security elements in the Intelligence Community for advice and support. This review should result in a complete rewrite of existing guidance and standards for the issuing, revoking, and suspending of security clearances. Special attention should be paid to establishing a clear—and relatively low—threshold for suspending clearances for cause, including pending criminal investigations.

The review also should significantly strengthen the background investigation process by restructuring contracts to create incentives for thoroughness. We strongly advocate abolishing the prevalent method of paying investigators "by the case." Strict "need-to-have" regulations should be issued for regular reviews of clearance requirements for all contract employees. Those without a continuing need should have their clearances withdrawn. The National Security Council should review and resolve issues on a government-wide basis that permit a person who is under FBI investigation for suspected espionage to obtain a new or renewed clearance; existing standards for clearance renewal also should be reviewed with an eye toward tightening up.

A Professional Administrative Inquiry Process. The agency Director should promulgate new agency guidelines and standards for security-related administrative inquiries to ensure that proper security/counterintelligence procedures and methods are employed. Very high professional qualification standards should be established and strictly maintained for all security personnel involved in administrative inquiries.

Physical/Technical/Cyber Security

Comprehensive Weapons Lab Cybersecurity Program. Under the sponsorship and specific guidance of the agency Director, the weapons labs should institute a broad and detailed program to protect all computer workstations, networks, links, and related systems from all forms of potential compromise. This program, which should be reviewed by and coordinated with appropriate offices within the US Intelligence Community, must include standard network monitoring tools and uniform configuration management practices. All lab computers and networks must be constantly monitored and inspected for possible compromise, preferably by an agency-sponsored, independent auditing body. The appropriate agency security authority should conduct on a yearly basis a "best practices" review.

Comprehensive Classified Document Control System. Document controls for the most sensitive data of the weapons labs should be re-instituted by the agency Director. The program should be constantly monitored by a centralized agency authority to ensure compliance.

Comprehensive Classification Review. The new agency, in coordination with the Intelligence Community, should promulgate new, concise, and precise classification guidance to define and ensure awareness of information and technologies

that require protection. This guidance should clear up the widespread confusion over what is export-controlled information; what information, when joined with other data, becomes classified; and the differences between similarly named and seemingly boundless categories such as "unclassified controlled nuclear information" and "sensitive but unclassified nuclear information."

Business Issues

Make Security an Integral Part of Doing Business. Security compliance must be a major requirement in every agency contract with the weapons labs. Rather than a detailed list of tasks, the contract should make clear the security and counterintelligence standards by which the lab will be held accountable. It is the responsibility of the lab to develop the means to achieve those objectives. If a lab fails to conform to these standards and requirements, the agency should withhold performance award fees.

Review the Process for Lab Management Contracts. If the agency director has reason to open the bidding for lab management contracts, we strongly recommend an intensive market research effort. Such an effort would help ensure that legitimate and competent bidders, with strong records for productive research and development, participate in the competition.

Weapons Labs Foreign Visitors Program. This productive program should continue, but both the agency and the weapons labs, in concert, must ensure that secret information is protected. This means precise policy standards promulgated by the agency to ensure: the integrity of the secure areas and control over all foreign visitors and assignees, a clear demarcation between secure and open areas at the labs, strong enforcement of restrictions against sensitive foreign visitors and assignees having access to secure facilities, and sensible but firm guidelines for weapons lab employees' contacts with foreign visitors from sensitive countries. Exceptions should be made by the agency director on a case-by-case basis. Clear, detailed standards should be enforced to determine whether foreign visits and appointments receive approval. The burden of proof should be placed on the employees who propose to host visitors from sensitive countries. Visits should be monitored by the labs and audited by an independent office. The bottom line: treat foreign visitors and assignees with the utmost courtesy, but assume they may well be collecting information for other governments.

Foreign Travel Notification. The agency should institute a program whereby all agency and weapons lab employees in designated sensitive positions must make written notification of official and personal foreign travel well before departure. The agency must keep close records of these notifications and also ensure that effective counterintelligence briefings are provided to all such travelers. Unless formally granted an exception, scientists for weapons labs should travel in pairs on official visits to sensitive countries.

Counterintelligence. The FBI should explore the possibility of expanding foreign counterintelligence resources in its field offices near the weapons labs.

Intelligence Community Damage Assessment of China's Acquisition of US Nuclear Weapons Information

Chinese strategic nuclear efforts have focused on developing and deploying a survivable long-range missile force that can hold a significant portion of the US and Russian populations at risk in a retaliatory strike. By at least the late 1970s, the Chinese launched an ambitious collection program focused on the United States, including its national laboratories, to acquire nuclear weapons technologies. By the 1980s, China recognized that its second strike capability might be in jeopardy unless its force became more survivable. This probably prompted the Chinese to heighten their interest in smaller and lighter nuclear weapon systems to permit a mobile force.

China obtained by espionage classified US nuclear weapons information that probably accelerated its program to develop future nuclear weapons. This collection program allowed China to focus

successfully down critical paths and avoid less promising approaches to nuclear weapons designs.

- China obtained at least basic design information on several modern US nuclear reentry vehicles, including the Trident II (W-88).

- China also obtained information on a variety of US weapon design concepts and weaponization features, including those of a neutron bomb.

- We cannot determine the full extent of weapon information obtained. For example, we do not know whether any weapon design documentation or blueprints were acquired.

- We believe it is more likely that the Chinese used US design information to inform their own program than to replicate US weapon designs.

China's technical advances have been made on the basis of classified and unclassified information deriving from espionage, contact with US and other countries' scientists, conferences and publications, unauthorized media enclosures, declassified US weapons information, and Chinese indigenous development. The relative contribution of each cannot be determined.

Regardless of the source of the weapons information, it has made an important contribution to the Chinese objective to maintain a second strike capability, and it has provided useful information for future designs.

Significant deficiencies remain in the Chinese weapons program. The Chinese almost certainly are using aggressive collection efforts to address deficiencies as well as to obtain manufacturing and production capabilities from both nuclear and non-nuclear sources.

To date, the aggressive Chinese collection effort has not resulted in any apparent modernization of their deployed strategic force or any new nuclear weapons deployment.

China has had the technical capability to develop a multiple independently targetable reentry vehicle (MIRV) system for its large, currently deployed ICBM for many years but has not done so. US information acquired by the Chinese could help them develop a MIRV for a future mobile missile.

We do not know if US classified nuclear information acquired by the Chinese has been passed to other countries. Having obtained more modern US nuclear technology, the Chinese might be less concerned about haring their older technology.

Endnotes

[1] The Department of Energy National Weapons Labs and Plants discussed in this report are Lawrence Livermore National Lab, California; Los Alamos National Lab, New Mexico; Sandia National Lab, New Mexico; PANTEX Plant, Texas; Kansas City Plant, Missouri; Oak Ridge (Y-12) Plant, Tennessee.

[2] US Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998.

[3] US Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998.

[4] Classified DOE report.

[5] Classified DOE report.

[6] Classified DOE report.

[7] Classified DOE report.

[8] DOE, Office of Counterintelligence, "The Foreign Intelligence Threat to Department of Energy Personnel, Facilities and Research, Summary Report," August 1990.

[9] Classified US Government report.

[10] GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997.

[11] Hewlett, Richard G., and Francis Duncan, "Atomic Shield: A History of the U.S. Atomic Energy Commission," May 1969.

[12] Classified DOE report.

[13] DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993

[14] Classified FBI report.

[15] Classified US Government report.

[16] Classified DOE report.

[17] DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994 (U).

[18] DOE/IG-385, "Special Audit Report on the Department of Energy's Arms and Military-Type Equipment," 1 February 1996.

[19] Classified DOE report.

[20] DOE, "Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," September 1996.

[21] GAO/RCED-91-12, "Nuclear Safety: Potential Security Weaknesses at Los Alamos and other DOE Facilities," October 1990 (U), and GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities,"13 December 1991.

[22] GAO/RCED-90-122, "Nuclear Security: DOE Oversight of Livermore's Property Management System is Inadequate," 18 April 1990.

[23] GAO/"Key Factors Underlying Security Problems at DOE Facilities" (Statement of Victor S. Rezendes, Director, Energy, Resources and Science Issues, Resources, Community, and Economic Development Division, GAO, in testimony before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives), 20 April 1999.

[24] Ibid.

[25] Classified DOE report.

[26] Hewlett, Richard G. and Francis Duncan, "Atomic Shield, A History of the United States Atomic Energy Commission," May 1969.

[27] GAO/RCED-89-34, "Nuclear Security: DOE Actions to Improve the Personnel Clearance Program," 9 November 1988.

[28] DOE/IG/WR-0-90-02, "Nevada Operations Office Oversight of Management and operating Contractor Security Clearances," March 1990.

[29] Classified DOE report.

[30] DOE/IG/WR-B-91-08, "Review of Contractor's Personnel Security Clearances at DOE Field Office, Albuquerque," September 1991.

[31] DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993.

[32] DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1995," January 1996.

[33] Classified US Government report.

[34] Classified DOE report.

[35] GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE Weapons Facilities," 13 December 1991.

[36] Classified DOE report.

[37] Classified DOE report.

[38] DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994. (U)

[39] DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1994," January 1995. (U)

[40] Classified DOE report.

[41] Classified DOE report.

[42] Classified DOE report.

[43] Classified DOE report.

[44] Classified DOE report.

[45] GAO/RCED-89-31, "Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories," 11 October 1988.

[46] Classified US Government report.
[47] GAO/RCED-97-229, "Department of Energy: DOE Needs To Improve Controls Over Foreign Visitors to Weapons Laboratories," 25 September 1997.
[48] Classified DOE report.
[49] GAO/RCED-97-229, "Department of Energy: DOE Needs To Improve Controls Over Foreign Visitors to Weapons Laboratories," 25 September 1997.
[50] Ibid.
[51] DOE, "Response to the Cox Committee Report: The Benefits of Department of Energy International Scientific and Technical Exchange Programs," April 1999.
[52] GAO/RCED-99-19, "Department of Energy: Problems in DOE's Foreign Visitors Program Persist," 6 October 1998.
[53] In April 1997, the FBI Director met with Secretary Pena, who had taken office in March, to deliver a highly critical FBI assessment of DOE's counterintelligence program. In June, DOE officials briefed the Special Assistant to the President and Senior Director for Nonproliferation and Export Controls. In July, the FBI Director and the Director of Central Intelligence expressed serious concern that DOE had not moved to implement the recommendations in the FBI report.
[54] The National Counterintelligence Policy Board (NACIPB) was created by a 1994 Presidential Decision Directive to serve as the National Security Council's primary mechanism to develop an effective national counterintelligence program. Current core NACIPB members include senior representatives from the Director of Central Intelligence/Central Intelligence Agency, the Federal Bureau of Investigation, the Department of Defense, the Department of State, the Department of Justice, the military departments' CI organizations, the National Security Council, and, as of 1997, the Department of Energy and NSA.

Central Intelligence Agency Inspector General

REPORT OF INVESTIGATION

IMPROPER HANDLING OF CLASSIFIED INFORMATION BY JOHN M. DEUTCH (1998-0028-IG)

February 18, 2000

L. Britt Snider
Inspector General

Daniel S. Seikaly
Assistant Inspector General for Investigations

This Report contains information that is or may be subject to the protections of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, or that otherwise may implicate the privacy interests of various current or former federal employees and private citizens.

This unclassified report has been prepared from the July 13, 1999 version of the classified Report of Investigation at the request of the Senate Select Committee on Intelligence. Information in this version is current as of the date of the original report. All classified information contained in the original Report of Investigation has been deleted.

INTRODUCTION

1. John M. Deutch held the position of Director of Central Intelligence (DCI) from May 10, 1995 until December 14, 1996. Several days after Deutch's official departure as DCI, classified material was discovered on Deutch's government-owned computer, located at his Bethesda, Maryland residence.

2. The computer had been designated for unclassified use only and was connected to a modem. This computer had been used to access [an Internet Service Provider (ISP)], the Internet, [Deutch's bank], and the Department of Defense (DoD). This report of investigation examines

Deutch's improper handling of classified information during his tenure as DCI and how CIA addressed this matter.

3. Currently, Deutch is a professor at the Massachusetts Institute of Technology. He also has two, no-fee contracts with the CIA. The first is to provide consulting services to the current DCI and his senior managers; this contract went into effect on December 16, 1996, has been renewed twice, and will expire in December 1999. The second contract is for Deutch's appointment to serve on the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (Proliferation Commission). Under the terms of the second contract, this appointment will continue until the termination of the Commission.

SUMMARY

4. The discovery of classified information on Deutch's unclassified computer on December 17,1996 was immediately brought to the attention of senior Agency managers. In January 1997, the Office of Personnel Security (OPS), Special Investigations Branch (SIB), was asked to conduct a security investigation of this matter.[1] A technical exploitation team, consisting of personnel expert in data recovery, retrieved the data from Deutch's unclassified magnetic media and computers. The results of the inquiry were presented to CIA senior management in the spring and summer of 1997.

5. The Office of General Counsel (OGC) had been informed immediately of the discovery of classified information on Deutch's computer. Although such a discovery could be expected to generate a crimes report to the Department of Justice (DoJ), OGC determined such a report was not necessary in this case. No other actions, including notification of the Intelligence Oversight Committees of the Congress[2] or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board, were taken until the Office of Inspector General (OIG) opened a formal investigation in March 1998. On March 19, 1998, OIG referred the matter to DoJ. On April 14,1999, the Attorney General declined prosecution and suggested a review to determine Deutch's suitability for continued access to classified information.

6. Deutch continuously processed classified information on government-owned desktop computers configured for unclassified use during his tenure as DCI. These unclassified computers were located in Deutch's Bethesda, Maryland and Belmont, Massachusetts residences,[3] his offices in the Old Executive Office Building (OEOB), and at CIA Headquarters. Deutch also used an Agency-issued unclassified laptop computer to process classified information. All were connected to or contained modems that allowed external connectivity to computer networks such as the Internet. Such computers are vulnerable to attacks by unauthorized persons. CIA personnel retrieved [classified] information from Deutch's unclassified computers and magnetic media related to covert action, Top Secret communications intelligence and the National Reconnaissance Program budget.

7. The OIG investigation has established that Deutch was aware of prohibitions relating to the use of unclassified computers for processing classified information. He was further aware of specific vulnerabilities related to the use of unclassified computers that were connected to the Internet. Despite this knowledge, Deutch processed a large volume of highly classified information on these unclassified computers, taking no steps to restrict unauthorized access to the information and thereby placing national security information at risk.

8. Furthermore, the OIG investigation noted anomalies in the way senior CIA officials responded to this matter. These anomalies include the failure to allow a formal interview of Deutch, and the absence of an appropriate process to review Deutch's suitability for continued access to classified information.

BACKGROUND

9. In 1998, during the course of an unrelated investigation, OIG became aware of additional circumstances surrounding an earlier allegation that in 1996 Deutch had mishandled classified information. According to the 1996 allegation, classified information was found on a computer configured for unclassified use at Deutch's Maryland residence. This computer had been used to connect to the Internet. Additionally, unsecured classified magnetic media was found in Deutch's study at the residence. Further investigation uncovered additional classified information on other Agency-owned unclassified computers issued to Deutch. In 1998, OIG learned that senior Agency officials were apprised of the results of the OPS investigation but did not take action to properly resolve this matter. The Inspector General initiated an independent investigation of Deutch's alleged mishandling of classified information and whether the matter was appropriately dealt with by senior Agency officials.

PROCEDURES AND RESOURCES

10. OIG assigned a Supervisory Investigator, five Special Investigators, a Research Assistant, and a Secretary to this investigation. The team of investigators interviewed more than 45 persons thought to possess knowledge pertinent to the investigation, including Deutch, DCI George Tenet, former CIA Executive Director Nora Slatkin, former CIA General Counsel Michael O'Neil, and [the] former FBI General Counsel. The team reviewed security files, memoranda for the record written contemporaneously with the events under investigation, data recovered from Deutch's unclassified magnetic media, Congressional testimony, and material related to cases involving other individuals who mishandled classified information. Pertinent information was also sought from the National Security Agency (NSA), the DoD, and an Internet service provider (ISP). In addition, the team reviewed applicable criminal statutes, Director of Central Intelligence Directives, and Agency rules and regulations.

QUESTIONS PRESENTED

11. This Report of Investigation addresses the following questions:

- Why was Deutch issued government computers configured for unclassified use and were his computer systems appropriately marked as unclassified?
- Why was Deutch permitted to retain government computers after resigning as DCI?
- What information was found on Deutch's magnetic media?
  - How was the classified material discovered?
  - What steps were taken to gather the material?
  - What steps were taken to recover information residing on Deutch's magnetic media?
  - What are some examples of the classified material that was found?
- What vulnerabilities may have allowed the hostile exploitation of Deutch's unprotected computer media?
  - What was the electronic vulnerability of Deutch's magnetic media?
  - What was the physical vulnerability of Deutch's magnetic media?
- Could it be determined if classified information on Deutch's unclassified computer was compromised?
- What knowledge did Deutch have concerning vulnerabilities associated with computers?
  - What is Deutch's recollection?
  - What did Deutch learn at [an] operational briefing?
  - What was Deutch's Congressional testimony?
  - What are the personal recollections of DCI staff members?
- Had Deutch previously been found to mishandle classified information?
- What laws, regulations, agreements, and policies have potential application?
- How was a similar case handled?
- What actions did senior Agency officials take in handling the Deutch case?
  - What actions were taken by senior Agency

officials after learning of this matter?
    - How were the Maryland Personal Computer Memory Card International Association (PCMCIA) cards handled?
    - What was the course of the Special Investigations Branch's investigation of Deutch?
- Should a crimes report initially have been filed on Deutch in this case?
- Should application of the Independent Counsel statute have been considered?
- Were senior Agency officials obligated to notify the Congressional oversight committees or the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board? Were these entities notified?
- Why was no administrative sanction imposed on Deutch?
- What was OIG's involvement in this case?
    - When did OIG first learn of this incident?
    - Why did OIG wait until March 1998 to open an investigation?
    - What steps were taken by OIG after opening its investigation?
- What is Deutch's current status with the CIA?
- What was the disposition of OIG's crimes report to the Department of Justice?

CHRONOLOGY OF SIGNIFICANT EVENTS

1995

January 1	John Deutch establishes Internet access via an [ISP provider].
May 10	Deutch sworn in as DCI.
June 15	Earliest classified document later recovered by technical exploitation team.
August 1	Deutch receives [a] briefing on computer attacks.

1996

December 5	Deutch requests that he be able to retain computers after he leaves office.
December 13	Deutch signs a no-fee-consulting contract permitting him to retain government computers.
December 14	Deutch's last day as DCI.
December 17	Classified information found on Deutch's computer in Bethesda, Maryland. Slatkin and O'Neil notified. Slatkin notifies Tenet within a day. O'Neil informs Deutch of discovery.
December 23	Four PCMCIA cards retrieved from Deutch and given to O'Neil.
December 27	Hard drive from Deutch's Maryland computer retrieved.
December 28	Chief/DCI Administration informs IG Hitz of discovery at Deutch's residence.
December 30	Hard drives from residences given to O'Neil.

1997

January 6	OPS/SIB initiates investigation on Deutch. PDGC and the OPS Legal Advisor discuss issue of a crimes report.
January 9	O'Neil releases to DDA Calder and C/SIB the hard drives from the residences and two of six PCMCIA cards. O'Neil retains four PCMCIA cards from the Maryland residence.
January 9	Memo from ADCI to D/OPS directing Deutch to keep clearances through December 1997.
January 13	Technical exploitation team begins the recovery process.

January 22	Technical exploitation team documents that two hard drives contain classified information and had Internet exposure after classified material placed on drives.
January 30	O'Neil speaks with FBI General Counsel and was reportedly told that FBI was not inclined to investigate.
February 3	O'Neil releases four remaining PCMCIA cards that are subsequently exploited.
February 21	C/SIB meets with OIG officials to discuss jurisdictional issues.
February 27	D/OPS tasked to review all material on hard drives and PCMCIA cards.
March 11	D/OPS completes review of 17,000 pages of recovered items.
July 8	D/OPS's report to ADCI prepared for distribution. Included on distribution are Slatkin, O'Neil, and Richard Calder.
July 21	Slatkin is replaced as Executive Director.
July 30	PDGC reaffirms with OGC attorney that original disks and hard drives need to be destroyed to ensure protection of Deutch's privacy.
August 11	PDGC appointed Acting General Counsel and O'Neil goes on extended annual leave.
August 12	Technical exploitation team confirms selected magnetic media were destroyedper instruction of D/OPS.
September 8	Slatkin leaves CIA.
October 1	O'Neil retires from CIA.
November 24	DCI approves Deutch and other members of the Proliferation Commission for temporary staff-like access to CIA information and facilities without polygraph.
1998	
February 6	OIG is made aware of additional details of the SIB investigation and subsequently opens a formal investigation.
March 19	IG forwards crimes report to DoJ.
May 8	IG letter to IOB concerning Deutch investigation.
June 2	DCI notifies oversight committees of investigation.
1999	
April 14	Attorney General Reno declines prosecution and suggests a review of Deutch'ssecurity clearances.

FINDINGS

WHY WAS DEUTCH ISSUED GOVERNMENT COMPUTERS CONFIGURED FOR UNCLASSIFIED USE AND WERE HIS COMPUTER SYSTEMS APPROPRIATELY MARKED AS UNCLASSIFIED?

12. The then-Chief of the Information Services Management Staff (C/ISMS) for the DCI Area, recalled that prior to Deutch's confirmation as DCI, she was contacted by [Deutch's Executive Assistant] regarding computer requirements for Deutch. C/ISMS, who would subsequently interface with [the Executive Assistant] on a routine basis, learned that

Deutch worked exclusively on Macintosh computers. An Information Security (Infosec) Officer assigned to ISMS recalled C/ISMS stating that [the Executive Assistant] instructed [her] to provide Internet service at the 7th floor Headquarters suite, OEOB, and Deutch's Maryland residence.

13. According to C/ISMS, Deutch's requirements, as imparted by [his Executive Assistant], were for Deutch to have not only access to the Internet, including electronic messaging, but access to CIA's classified computer network from Deutch's offices in CIA Headquarters, OEOB, and his Maryland residence. In addition, Deutch was to be issued an unclassified laptop with Internet capability for use when traveling.

14. A computer specialist, who had provided computer support to Deutch at the Office of the Secretary of Defense, confirmed that, at Deutch's request, he had been hired by CIA to establish the same level of computer support Deutch had received at the Pentagon. At CIA, the computer specialist provided regular and close computer support to Deutch on an average of once a week. The computer specialist recalled [that Deutch's Executive Assistant] relayed that he and Deutch had discussed the issue of installing the classified computer at Deutch's Maryland residence, and Deutch either did not believe he needed or was not comfortable having the classified computer in his home.

15. [Deutch's Executive Assistant] also remembered discussions about locating a classified computer at Deutch's Maryland residence. [The Executive Assistant], however, could not recall with any certainty if the computer had in fact been installed. [The Executive Assistant] said that a classified system had been installed at his own residence. However, after using it once, he found its operation to be difficult and time consuming, and he had it removed from his residence. [The Executive Assistant's] experience with the deployed classified system may have influenced Deutch to decide he did not want one located at his Maryland residence. If so, [the Executive Assistant] would have informed the ISMS representative of Deutch's decision.

16. C/ISMS recalled [the Executive Assistant] telling her he was not sure Deutch required a classified computer system at Deutch's Maryland residence.

17. A Local Area Network (LAN) technician installed classified and unclassified Macintosh computers in Deutch's 7th floor Headquarters office and in Deutch's OEOB office. The technician also installed a computer configured for unclassified use at Deutch's Maryland residence. The technician stated that Deutch was also provided with an unclassified laptop that had an internal hard drive with modem and Internet access. The computer specialist installed an unclassified computer at Deutch's Belmont residence several months after Deutch was appointed DCI.

18. Personal Computer Memory Card International Association (PCMCIA) cards are magnetic media capable of storing large amounts of data. According to the computer specialist, Deutch's unclassified computers were equipped with PCMCIA card readers. The computer specialist said this configuration afforded Deutch the opportunity to write to the cards and back up information. One PCMCIA card would reside at all times in a reader that was attached to the unclassified computer, and the other PCMCIA card would be in Deutch's possession. The computer specialist stated that Deutch valued the ability to access, at several locations, data on which he was working. C/ISMS stated that all the unclassified computers and PCMCIA cards provided for Deutch's use contained a green label indicating the equipment was for unclassified purposes. The LAN technician also stated that a concern was to label all of Deutch's automated data processing equipment and magnetic media, including

monitors and PCMCIA cards, as either "unclassified" (green label) or "Top Secret" (purple label). The technician stated that his purpose was to make it perfectly clear to Deutch and anyone else using these systems, what was for classified and unclassified use.

19. The OIG has in its possession eight PCMCIA cards that had been used by Deutch. Seven of the eight cards were labeled unclassified; the eighth was not labeled. Four of the cards were from the Maryland residence. Three of the cards were from CIA Headquarters and one was from the OEOB. In addition, OIG received four Macintosh computers and one Macintosh laptop that were used by Deutch. The laptop and two of the computers were marked with green unclassified labels; the other two computers were marked with purple classified labels. One of the classified computers was determined to have come from Deutch's 7th floor Headquarters office; the other from his OEOB office.

WHY WAS DEUTCH PERMITTED TO RETAIN GOVERNMENT COMPUTERS AFTER RESIGNING AS DCI?

20. In a Memorandum for the Record (MFR) dated December 30, 1996, [the] then Chief DCI Administration (C/DCI Administration), noted that Deutch announced on December 5, 1996 that he would resign as DCI. That same day, according to C/DCI Administration's MFR, Deutch summoned [him] to his office. Deutch told [him] "to look at a way in which he could keep his government computers."

21. The C/DCI Administration's MFR indicated that on December 6, 1996, he spoke with [the then] Chief of the Administrative Law Division[4] (C/ALD) in OGC, to ask if Deutch could retain his Agency-issued, unclassified computer after leaving CIA. C/ALD reportedly said that he had concerns with government-owned property that was to be utilized for personal use. He advised that he would discuss the matter with the Principal Deputy General Counsel (PDGC).

22. On December 9, 1996, C/DCI Administration asked ISMS personnel to identify a system configuration which was identical to Deutch's. [He] hoped that Deutch would purchase a computer instead of retaining a government-owned computer.

23. According to a December 19, 1996 MFR signed by C/ALD and the PDGC, [C/ALD] discussed with [her] the request to loan computers to Deutch.[5] [She] mentioned the request to General Counsel Michael O'Neil, and stated:

    The only legal way to loan the computers to the DCI would be if a contract was signed setting forth that John Deutch was a consultant to the CIA, and that the computers were being loaned to Mr. Deutch to be used solely for U.S. Government business.

24. Despite her reservations, the PDGC was told by O'Neil to work with C/DCI Administration to formulate a contract for Deutch to be an unpaid consultant. The contract would authorize the provision of a laptop computer for three months and a desktop computer for up to a year.

25. According to the MFR:

    On or about 11 December, [the PDGC] was informed by [C/DCI Administration] that the DO wanted the computers loaned to him because they had the DO's personal financial data on them and he wanted access to that data. [C/DCI Administration] learned this information in conversation with the DCI. [The PDGC] informed [C/ALD] of this development, and they both agreed that it was improper to loan the computers to the DCI if the true purpose of the loan was to allow the DCI to have continued access to his personal information. [The PDGC] and [C/ALD] also expressed concern that the computers should not have been used by the DCI to store personal financial records since this would constitute improper use of a government computer. [C/

ALD] held further conversations with [C/DCI Administration] at which time [C/ALD] suggested that the DCI's personal financial data be transferred to the DCI's personal computer rather than loaning Agency computers to the DCI. [C/DCI Administration] stated that this proposal would not work because the DCI did not own any personal computers. It was then suggested that the DCI be encouraged to purchase a personal computer and that the DCI personal financial records be transferred to the computer.

26. On December 10, 1996, a no-fee contract was prepared between John Deutch, Independent Contractor, and the CIA. Deutch was to provide consulting services to the DCI and senior managers, was to retain an Agency-issued laptop computer for three months, and would retain an Agency-issued desktop computer for official use for one year.

27. C/DCI Administration's MFR notes that on December 13,1996, he spoke with O'Neil on the telephone. O'Neil directed that the contract being prepared for Deutch be modified to authorize Deutch two computers for a period of one year. The contract was revised on December 13, 1996; the reference to the laptop was deleted but Deutch was to retain two Agency-issued desktop computers and two STU-III secure telephones for one year.

28. According to the C/DCI Administration's MFR, on December 12, 1996, [he] again met with Deutch to discuss matters relating to Deutch's departure. The computer issue was again discussed:

I mentioned again that I had "strong reservations" about Mr. Deutch maintaining the Government-owned computers and restated that we would be happy to assist moving Mr. Deutch to a personally-owned platform. Mr. Deutch slammed shut his pen drawer on his desk and said thanks for everything without addressing the issue.

29. According to the C/ALD and PDGC MFR, they met with O'Neil on December 13, 1996 to discuss the loan of the computers to Deutch. [They] expressed concern that the loan of the computers would be improper if Deutch intended to use the computers for personal purposes. O'Neil stated that he had discussed the matter with Deutch, and Deutch knew he could not use the computers for personal purposes. O'Neil also stated, according to the MFR, that Deutch had his own personal computers and that Deutch would transfer any personal data from the CIA computers to his own. O'Neil said that the contract, which only called for the loan of two computers, had to be re-drafted so that it would cover the loan of a third computer. O'Neil advised that Deutch would not agree to an arrangement in which he would simply use his own computers for official work in place of a loaned CIA computer.[6]

30. The PDGC recalls standing in the receiving line at a farewell function for Deutch and being told by Deutch's wife, "I can't believe you expect us to go out and buy another computer."

31. The MFR indicates that [the two OGC attorneys] dropped their objections to the loan of the computers, based on assurances from O'Neil that Deutch understood the computers would only be used for official purposes, and he would transfer his personal financial data to his own computer.

32. The contract was signed on December 13, 1996 by O'Neil and Deutch. The effective date for the contract was December 16, 1996. The contract states that Deutch "shall retain, for Government use only, two (2) Agency-issued desktop computers and two (2) STU-III's for the period of one year." Instead, Deutch was issued three PCMCIA cards and two PCMCIA card readers and all government-owned computers were returned to the Agency. On June 23, 1997, he purchased the cards and readers from CIA for $1,476.

WHAT INFORMATION WAS FOUND ON DEUTCH'S MAGNETIC MEDIA?

How was the classified material discovered?

33. Each of the two, unclassified, Agency-owned computers that were to be loaned to Deutch under the provisions of the December 13, 1996 contract were already located at Deutch's Maryland and Belmont residences. To effect the loan of the computers, C/DCI Administration, after consulting with Deutch and his personal assistant, requested that an Infosec Officer perform an inventory of the two government-owned Macintosh computers and peripherals at the Deutch residences. In addition, the Infosec Officer was to do a review to ensure no classified material had been accidentally stored on these computers. While at the Deutch residences, a contract engineer was to document the software applications residing on the computers and, at Deutch's request, install several software applications. This software included FileMaker Pro (e.g., a database) that was to be used with a calendar function and Lotus Notes that would be used with an address book. Deutch has no recollection of authorizing an inventory or a personal visit to his residences and questions the appropriateness of such a visit.

34. On December 17, 1996, the contract network engineer and the Infosec Officer, escorted by a member of the DCI security protective staff, entered Deutch's Maryland residence to conduct the review of the unclassified Macintosh computer and its peripherals. The Infosec Officer reviewed selected data on the computer and two PCMCIA cards, labeled unclassified, located in each of two PCMCIA card drives. Two other PCMCIA cards, one labeled unclassified and the other not labeled, were located on Deutch's desk.

35. The Infosec Officer's initial review located six files containing what appeared to be sensitive or classified information. Although the Infosec Officer believed that numerous other classified or sensitive files were residing on the computer, he concluded the system was now classified and halted his review. The contract network engineer agreed the system should be considered classified based on the information residing on the computer.

36. In addition to these six files, the contract network engineer and the Infosec Officer noted applications that allowed the Macintosh computer external connectivity via a FAX modem. The computer also had accessed the Internet via [an ISP], a DoD unclassified e-mail system, and [Deutch's bank] via its proprietary dial-up software.

What steps were taken to gather the material?

37. The Infosec Officer telephoned C/DCI Administration and informed him of the discovery of classified material. Although normal information security practice would have been to immediately confiscate the classified material and equipment, C/DCI Administration advised the Infosec Officer to await further instruction. [He] proceeded to contact then-CIA Executive Director Nora Slatkin. She referred him to O'Neil for guidance. [He] stated that he consulted with O'Neil, who "requested that we print off copies of the documents for his review." [He] contacted the Infosec Officer and instructed him to copy the six classified/sensitive files to a separate disk and return to Headquarters. The Infosec Officer copied five of the six files.[7]

38. After returning to Headquarters, the contract network engineer recalled being contacted by O'Neil. O'Neil advised that he had spoken with Deutch, and Deutch could not understand how classified information came to be found on the computer's hard drive. O'Neil wanted to know if any extraordinary measures were used to retrieve the classified documents

and was told the documents were simply opened using Microsoft Word. O'Neil asked the contract network engineer to wait while Deutch was again contacted.

39. Shortly thereafter, the contract engineer stated that Deutch telephoned him and said he could not understand how classified information could have been found on the computer's hard drive as he had stored such information on the PCMCIA cards. The contract engineer told Deutch that the classified information had been found on the PCMCIA cards. The contract engineer recalled suggesting that Deutch might want a new hard drive and replacement PCMCIA cards to store unclassified files that could be securely copied from Deutch's existing PCMCIA cards. According to the contract engineer, Deutch agreed but wanted to review the PCMCIA card files first because they contained personal information.

40. On December 23, 1996, Deutch provided the four PCMCIA cards from his Maryland residence to the DCI Security Staff. These four cards were delivered to O'Neil the same day.

41. On December 27, 1996, the contract network engineer advised C/DCI Administration that two PCMCIA cards previously used by Deutch had been located in an office at Headquarters. One of the cards had an unclassified sticker and was labeled as "Deutch's Personal Disk." The other did not have either a classification sticker or a label. The files on the card with the unclassified sticker had been erased; however, the contract network engineer was able to recover data by the use of a commercially available software utility. Although labeled "unclassified," the contract network engineer noted that the files contained words such as "Secret," "Top Secret Codeword," "CIA," and the name of an Office of Development and Engineering facility. This discovery caused C/DCI Administration, on the advice of [the] Associate Deputy Director for Administration (ADDA),[8] to contact O'Neil for assistance in expeditiously retrieving Deutch's Macintosh computers from the Maryland and Belmont residences.

42. On the evening of December 27, 1996, the contract network engineer visited Deutch's Maryland residence, removed Deutch's hard drive, and delivered it to C/DCI Administration. On December 30, 1996, DCI Security Staff delivered to C/DCI Administration the hard drive from Deutch's Belmont residence. Both hard drives were then delivered to O'Neil.

43. On January 6, 1997, OPS/SIB, upon the approval of Slatkin, initiated an internal investigation to determine the security implications of the mishandling of classified information by Deutch.

44. According to Slatkin, she, O'Neil, and Richard Calder, Deputy Director for Administration had several discussions about how to proceed with the investigation. She also discussed with Acting DCI Tenet the issue of how to proceed. As a result, a select group was created to address this matter. Its purpose was to (1) take custody of the magnetic media that had been used by Deutch, (2) review Deutch's unclassified magnetic media for classified data, (3) investigate whether and to what extent Deutch mishandled classified information, and (4) determine whether classified information on Deutch's computers that had Internet connectivity was compromised.

45. By January 13, 1997, all hardware and files that had been used by Deutch, except four PCMCIA cards retrieved from Deutch's Maryland residence on December 23, 1996, were in SIB's possession. On February 3, 1997, O'Neil released the four PCMCIA cards to Calder, who transferred them to the group on February 4, 1997. Then-Director of Personnel Security (D/OPS) headed the group. Calder was the senior focal point for

the group. In addition, a technical exploitation team was formed to exploit the magnetic media.

What steps were taken to recover information residing on Deutch's magnetic media?

46. Five government-issued MacIntosh computer hard drives and eight PCMCIA cards, used by Deutch and designated for unclassified purposes, were examined by a technical exploitation team within the group. Because each of the computers had modems, the PCMCIA cards were considered equally vulnerable when inserted into the card readers attached to the computers. The group had concerns that the processing of classified information on Deutch's five computers that were designated for unclassified information were vulnerable to hostile exploitation because of the modems. The group sought to determine what data resided on the magnetic media and whether CIA information had been compromised.

47. The examination of Deutch's magnetic media was conducted during the period January 10 through March 11, 1997. The technical exploitation team consisted of a Senior Scientist and two Technical Staff Officers, whose regular employment responsibilities concerned [data recovery]. The Infosec Officer who participated in the December 17, 1996 security inspection at Deutch's Maryland residence also assisted in the exploitation effort.

48. This team performed the technical exploitation of Deutch's magnetic media, recovered full and partial documents containing classified information, and printed the material for subsequent review. Technical exploitation began with scanning for viruses and making an exact copy of each piece of media used by Deutch. Further exploitation was performed on the copies. The original hard drives and PCMCIA cards were secured in safes. The copies were restored, in a read-only mode, on computers used by the team. Commercially available utility software was used to locate, restore, and print recoverable text files that had been erased. In an attempt to be exhaustive, the Senior Scientist wrote a software program to organize text fragments that appeared to have been part of word processing documents.

49. To accommodate concerns for Deutch's privacy, D/OPS was selected to singularly review all recovered data. He reviewed in excess of 17,000 pages of recovered text to determine which documents should be retained for possible future use in matters relating to the unauthorized disclosure of classified information.

50. Three of the PCMCIA cards surrendered by Deutch subsequent to the security inspection of December 17, 1996, were found to have characteristics that affected exploitation efforts. Specifically, the card labeled "John Backup" could not be fully exploited as 67 percent of the data was unrecognizable due to "reading" errors. The card labeled "Deutch's Disk" was found to have 1,083 "items" that were erased. The last folder activity for this card occurred on "December 20, 1996 at 5:51 [p.m.]." The third card, labeled "Deutch's Backup Disk" and containing files observed during the security inspection, was found to have been reformatted.[9] The card was last modified on "December 20,1996, [at] 5:19 p.m."

51. Subsequent investigation by OIG revealed that Deutch had paged the contract network engineer at 1000 hours on Saturday, December 21, 1996. In an e-mail to C/DCI Administration the following day, the contract network engineer wrote:

... he [Deutch] was experiencing a problem deleting files from one or [sic] his 170MB PCMCIA disks. As near as I [Contractor] can tell the disk has become corrupted and while it appears to allow him [Deutch] to copy files it did not allow him to delete them. We tried several techniques to get around the problem

but none were successful. He [Deutch] indicated that he [Deutch] would continue to copy files and not worry about deleting any additional files. He [Deutch] asked what we were going to do with the disks he returned and I told him that we would in all probability degauss them and then physically destroy them....

52. The exploitation efforts resulted in eight pieces of magnetic media yielding classified information. Of the eight pieces, four computers and three PCMCIA cards had prominent markings indicating that the equipment was for unclassified use.[10] Forty-two complete documents [were classified up to Top Secret and a non-CIA controlled compartmented program] and 32 text or document fragments classified up to [Top Secret and a non-CIA controlled compartmented program] were recovered. Fourteen of the recovered classified documents contained actual printed classification markings (i.e., "SECRET," "Top Secret/ [a non-CIA controlled compartmented program]") as part of the document. These documents were located on hard drives and/or PCMCIA cards linked to Deutch's residences, 7th floor CIA office, and laptop.

53. Indications of Internet, [an ISP],[11] an unclassified Pentagon computer e-mail,[12] and online banking usage were found on several of the storage devices. A virus was found to have corrupted a file on the computer formerly located in Deutch's 7th floor CIA office. This computer was labeled "DCI's Internet Station Unclassified," but yielded classified information during the exploitation effort.

54. Recovered computer-generated activity logs reflect, in certain instances, classified documents were created by "John Deutch" during the period of June 1, 1995 and November 14, 1996. Many of the same documents, in varying degrees of completion, were found on different pieces of magnetic media. Additionally, the team recovered journals (26 volumes) of daily activities maintained by Deutch while he served at the DoD and CIA.

55. The following text box provides a summary of Deutch's magnetic media that resulted in the recovery of classified information.

Media/Location	Markings	Connected To	Information Recovered
Quatum ProDrive Hard Drive/Deutch's Maryland Residence	"Unclassified" on MacIntosh Power PC	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet (ISP), (Deutch's bank), and DoD electronic mail usage. Indicators of visits to high risk Internet sites.[13]
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Disk," "Unclassified," GS001490	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	Three complete classified documents and text fragments including TS/Codeword.[14] (Bank) online usage. Card apparently reformatted on 12/20/96 at 5:51 p.m.
Microtech PCMCIA Card/Deutch's Maryland Residence	"Deutch's Backup Disk," "Unclassified," GS001490	PCMCIA Card Reader Networked to U.S. Robotics Fax Modem	31 complete classified documents and text fragements, five observed during security inspection. (Bank) Online Usage. Card apparently reformatted on 12/20/96 at 5:19 p.m.
Quatum ProDrive Hard Drive/Deutch's Belmont Residence	"JMD" on Drive Shell	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Six complete classified documents and text fragments including TS/Codeword. Internet usage. Indicators of visits to high risk Internet sites.
MacIntosh Power PC with Hard Drvie/Deutch's 7th Floor Office, Original Headquarters Building	"Unclassified," "Property of O/DI. . ." "DCI's Internet Station" Unclassified	U.S. Robotics Fax Modem Two PCMCIA Card Readers	One complete classified document and text fragements including TS/Codeword. Word macro concept virus. Internet, DoD electronic mail usage.
MacIntosh Power PC with Hard Drvie/ Deutch's OEOB	"Unclassified," "Property of DCI. . ."	U.S. Robotics Fax Modem Two PCMCIA Card Readers	Text fragements including TS/Codeword. DoD electronic mail usage.
MacIntosh Powerbook Laptop	"Dr. Deutch Primary" "Unclassified"	Global Village Internal Modem	Two complete classified documents and text fragments including TS/Codeword.
	"Property of DCI. . ."		
Microtech PCMICA Card/ISMS Office	"Deutch's Personal Disk," "Unclassified"	N/A	Text fragments including TS/Codeword.

What are some examples of the classified material that was found?

56. An October 7, 1996 memorandum from Deutch to the President and the Vice President, found on the hard drive of the Maryland residence computer [contained information at the Top Secret/Codeword level]. The last paragraph of the memorandum notes [that the information is most sensitive and must not be compromised]:

    Accordingly, with (National Security Advisor] Tony's [Lake] advice, I have restricted distribution of this information to Chris [Secretary of State Warren Christopher], Bill [Secretary of Defense William Perry], Tony [Lake], Sandy [Deputy National Security Advisor Sandy Berger], Leon Fuerth [the VP's National Security Advisor], and Louie Freeh with whom I remain in close touch.

57. [The] former Chief of Staff to the DCI and Slatkin both identified the memorandum as one Deutch composed on the computer at his Maryland residence in their presence on October 5, 1996.

58. In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch described an official trip. [The memorandum discussed information classified at the Top Secret level.]

59. In a memorandum to the President, which was found on a PCMCIA card from the Maryland residence, concerning a trip Deutch [discusses information classified at the Top Secret/ Codeword level].

60. Deutch's memorandum to the President found on a PCMCIA card from the Maryland residence also [discusses a non-CIA controlled compartmented program].

61. An undated memorandum from Deutch to the President that was found on a PCMCIA card from the Maryland residence discusses a trip. [The memorandum discusses information classified at the Secret level.]

62. Another Deutch memorandum to the President that was found on a PCMCIA card from the Maryland residence [discusses information classified at the Secret/Codeword level].

63. In a memorandum to the President that was found on a PCMCIA card from the Maryland residence, Deutch [discusses information classified at the Top Secret/Codeword level].

64. [In] a memorandum with no addressee or originator listed, noted as revised on May 9, 1996 that was found on a PCMCIA card from the Maryland residence, [Deutch discusses information at the Secret level].

65. A document with no heading or date concerning a Deutch trip was found on the hard drive of Deutch's laptop computer, which was marked for unclassified use, describes [information classified at the Secret/Codeword level].

66. A document without headings or dates, which was found on the hard drive of the unclassified computer in Deutch's 7th floor office, [discusses information classified at the Secret/ Codeword level].

67. Deutch's journal, which was found on a PCMCIA card from the Maryland residence, also covered this topic but in more detail.

68. A spread sheet document [contains] financial [data] from fiscal year 1995 (FY95) through FY01 [which is classified at the Secret/ compartmented program level. It was found on a PCMCIA card from the Maryland residence.

WHAT VULNERABILITIES MAY HAVE ALLOWED THE HOSTILE EXPLOITATION OF DEUTCH'S UNPROTECTED COMPUTER MEDIA?

69. The June 1994 User's Guide for PC Security, prepared by CIA's Infosec Officer Services Division, defines unclassified media as media that has never contained classified data. To maintain this status, all media and supplies related to an unclassified computer must be maintained separately from classified computer hardware, media, and supplies. Classified media is defined as media that contains or has contained classified data. It must be appropriately safeguarded from unauthorized physical (i.e., actually handling the computer) and electronic access (i.e., electronic insertion of exploitation software) that would facilitate exploitation. Computer media must be treated according to the highest classification of data ever contained on the media.

70. The Guide addresses vulnerabilities relating to computers. Word processors, other software applications, and underlying operating systems create temporary files on internal and external hard drives or their equivalents (i.e., PCMCIA cards). These temporary files are automatically created to gain additional memory for an application. When no longer needed for memory purposes, the location of the files and the data saved on the media is no longer tracked by the computer. However, the data continues to exist and is available for future recovery or unwitting transfer to other media.

71. Additionally, data contained in documents or files that are deleted by the user in a standard fashion continue to reside on magnetic media until appropriately overwritten. These deleted files and documents can be recovered with commercially available software utilities. Furthermore, computers reuse memory buffers, disk cache, and other memory and media locations (i.e., slack and free space) on storage devices without clearing all previously stored information. This results in residual data being saved in storage space allocated to new documents and files. Although this data cannot be viewed with standard software applications, it remains in memory and can be recovered.

72. As a result of these vulnerabilities, security guidelines mandate procedures to prevent unauthorized physical and electronic access to classified information. An elementary practice is to separately process classified and unclassified information. Hard drives, floppy disks, or their equivalents used in the processing of classified information must be secured in approved safes and areas approved for secure storage when not in use. Individuals having access to media that has processed classified information must possess the appropriate security clearance. Computers that process classified information and are connected to a dial-up telephone line must be protected with a cryptographic device (e.g., STU-III) approved by NSA.

What was the electronic vulnerability of Deutch's magnetic media?

73. Deutch used five government-owned Macintosh computers, configured for unclassified purposes, to process classified information. At least four of these computers were connected to modems that were lacking cryptographic devices and linked to the Internet, [an ISP], a DoD electronic mail server, and/or [bank] computers. As a result, classified information residing on Deutch's computers was vulnerable to possible electronic access and exploitation.

74. Deutch did receive e-mail on unclassified computers. One such message from France, dated July 11, 1995, was apparently from a former academic colleague who claimed to be a Russian.

75. Deutch's online identities used during his tenure as DO may have increased the risk of electronic attack. As a private subscriber [to an ISP], Deutch used a variant of his name for online identification purposes. He was also listed by true name in [the ISP's] publicly available online membership directory. This directory reflected Deutch as a user of Macintosh computers, a scientist, and as living

in Bethesda, Maryland. Similarly, Deutch's online identity associated with CIA was:

> johnd@odci[Office of DCI].gov[Government]

and with DoD, as:

> deutch.johnd@odsdpo[Office of Deputy Secretary of DefensePostOffice].secdef[Secretary of Defense].osd.mil[Military].

After his confirmation as DCI, Deutch's DoD user identity was unobtainable from their global address database.

76. The technical exploitation team determined that high risk Internet sites had placed "cookies"[15] on the hard drives of the computers from Deutch's residences. According to DDA Calder, SIB's investigation demonstrated that the high risk material was accessed when Deutch was not present. These web sites were considered "risky" because of additional security concerns related to possible technical penetration.

What was the physical vulnerability of Deutch's magnetic media?

77. Deutch's government-issued computer at his primary residence in Maryland contained an internal hard drive and was lacking password protection. The drive was not configured for removal and secure storage when unattended even though classified information resided on the drive. Additionally, at the time of the December 17, 1996 security inspection, three of the four unsecured PCMCIA cards yielded classified information: two in PCMCIA readers and one on the desk in Deutch's study. An empty safe was also found with its drawer open.

78. Unlike his predecessors, Deutch declined a 24-hour security presence in his residence, citing concerns for personal privacy. Past practice for security staff, if present in a DCI's residence, was to assume responsibility for securing classified information and magnetic media. To compensate for the lack of an in-house presence, CIA security personnel and local police drove by Deutch's residence on a periodic basis. The two security chiefs responsible for Deutch's protective detail stated that Deutch was responsible for securing classified information in his residence. Deutch said that he thought his residence was secure. In hindsight, he said that belief was not well founded. He said he relied, perhaps excessively, on the CIA staff and security officials to help him avoid mistakes that could result in the unauthorized disclosure of classified information.

79. On May 16, 1995, Deutch approved the installation of a residential alarm system to include an alarm on the study closet. A one-drawer safe was placed in the alarmed closet. These upgrades were completed by early June 1995.

80. According to the first Security Chief assigned to Deutch, the alarm deactivation [was provided] code to a resident alien who performed domestic work at the Maryland residence. The alien [was permitted] independent access to the residence while the Deutch's were away. CIA security database records do not reflect any security clearances being issued to the alien. The resident alien obtained U.S. citizenship during 1998.

COULD IT BE DETERMINED IF CLASSIFIED INFORMATION ON DEUTCH'S UNCLASSIFIED COMPUTER WAS COMPROMISED?

81. According to the Senior Scientist who led the technical exploitation team, there was "no clear evidence" that a compromise had occurred to information residing on storage devices used by Deutch. In a February 14, 1997 MFR, the Senior Scientist concluded:

> *A complete, definitive analysis, should one be warranted, would likely take many months or*

longer and still not surface evidence of a data compromise.

82. On May 2,1997, the Chief, SIB wrote in a memorandum to the Director of OPS:

In consultation with technical experts, OPS investigators determined the likelihood of compromise was actually greater via a hostile entry operation into one of Mr. Deutch's two homes (Bethesda, Maryland and Boston, Massachusetts) to "image" the contents of the affected hard drives .... Due to the paucity of physical security, it is stipulated that such an entry operation would not have posed a particularly difficult challenge had a sophisticated operation been launched by opposition forces .... The Agency computer experts advised that, given physical access to the computers, a complete "image" of the hard drives could be made in [a short amount of time].

WHAT KNOWLEDGE DID DEUTCH HAVE CONCERNING VULNERABILITIES ASSOCIATED WITH COMPUTERS?

What is Deutch's recollection?

83. During an interview with OIG, Deutch advised that, to the best of his recollection, no CIA officials had discussed with him the proper or improper use of classified and unclassified computers. Around December 1997, approximately one year after he resigned as DCI, he first became aware that computers were vulnerable to electronic attack. Not until that time, Deutch commented, had he appreciated the security risks associated with the use of a modem or the Internet in facilitating an electronic attack.[16]

84. Although stating that he had not received any CIA security briefings relating to the processing of information on computers, Deutch acknowledged that classified information must be properly secured when unattended. Specifically, he stated, "I am completely conscious of the need to protect classified information."

85. In response to being advised that classified information had been recovered from government computers configured for his unclassified work, Deutch stated that he "fell into the habit of using the [CIA] unclassified system [computers] in an inappropriate fashion." He specifically indicated his regret for improperly processing classified information on the government-issued Macintosh computers that were connected to modems. Deutch acknowledged that he used these government-issued computers to access [the ISP], [his bank], the Internet, and a DoD electronic mail server.

86. Deutch indicated he had become accustomed to exclusively using an unclassified Macintosh computer while serving at DoD. He acknowledged that prior to becoming DCI, he was aware of the security principle requiring the physical separation of classified and unclassified computers and their respective information. However, he said he believed that when a file or document was deleted (i.e., dragged to the desktop trash folder), the information no longer resided on the magnetic media nor was it recoverable. Deutch maintained that it was his usual practice to create a document on his desktop computers, copy the document to an external storage device (e.g., floppy disk), and drag the initial document to the trash folder.

87. During his tenure as DCI, Deutch said that he intentionally created the most sensitive of documents on computers configured for unclassified use. Deutch stated that if these documents were created on the classified CIA computer network, CIA officials might access the system at night and inappropriately review the information. Deutch said that he had not spent a significant amount of time thinking about computer security issues.

88. Deutch advised that other individuals had

used the government computer located in the study of his Maryland residence. Deutch's wife used this computer to prepare reports relating to official travel with her husband. Additionally, [another family member] used this computer to access [a university] library. Regarding the resident alien employed at the Maryland residence, Deutch indicated that, to his knowledge, this individual never went into the study. He further believed that the resident alien normally worked while Mrs. Deutch was in the residence.

What did Deutch learn at [an] operational briefing?

89. On August 1, 1995, Deutch and several senior CIA officials receive[d] various operational briefings.

90. [During these briefings] Deutch was specifically told that data residing on a [commercial ISP network was vulnerable to a computer attack.]

91. Deutch did not have a specific recollection relating to the August 1, 1995 briefing. He could not recall making specific comments to briefers concerning his use of [his ISP] and the need to switch to another ISP.

What was Deutch's Congressional testimony?

92. On February 22, 1996, DCI Deutch testified before the Senate Select Committee on Intelligence on the subject of worldwide security threats to the United States during the post-Cold War era. During his appearance, Deutch stated:

Mr. Chairman, I conclude with the growing challenge of the security of our information systems. There are new threats that come from changing technologies. One that is of particular concern to me is the growing ease of penetration of our interlocked computer and telecommunications systems, and the intelligence community must be in the future alert to these needs--alert to these threats.

93. On June 25, 1996, DCI Deutch testified in front of the Permanent Investigations Subcommittee of the Senate Governmental Affairs Committee. The Committee was investigating the vulnerability of government information systems to computer attacks. Deutch's testimony focused on information warfare, which he defined as unauthorized foreign penetrations and/or manipulation of telecommunications and computer network systems.

94. In his prepared statement submitted to the Committee, Deutch indicated:

like many others in this room, [I] am concerned that this connectivity and dependency [on information systems] make us vulnerable to a variety of information warfare attacks ....These information attacks, in whatever form, could ... seriously jeopardize our national or economic security .... I believe steps need to be taken to address information system vulnerabilities and efforts to exploit them. We must think carefully about the kinds of attackers that might use information warfare techniques, their targets, objectives, and methods .... Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation or foreign terrorist organization that is interested in developing an information warfare capability .... We have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks.

What are the personal recollections of DCI staff members?

95. Deutch's [Executive] Assistant served in that position from February 1995 through July 1996 at DoD and CIA. [He] considered Deutch to be an "expert" computer user. [The Executive Assistant] was responsible for coordinating the preparation of computers for Deutch's use upon

his confirmation as DCI. During the transition, [the Executive Assistant] informed Deutch that the processing of classified and unclassified information required the use of separate computers to prevent the improper transfer of data. [The Executive Assistant] stated that the computer support staff at CIA went to great lengths to appropriately label Deutch's computers as either classified or unclassified in order to prevent improper use.

96. [The Executive Assistant] advised that he never informed Deutch that it was permissible to process classified information on a computer configured for unclassified use. [The Executive Assistant] stated that he was not aware that Deutch processed classified information on computers configured for unclassified use. When advised that classified material had been recovered from multiple computers used by Deutch that had been configured for unclassified purposes, [the Executive Assistant] responded that he was at a loss to explain why this had occurred.

97. [The Executive Assistant] remembered the August 1, 1995 briefing. [The Executive Assistant] said that Deutch was very concerned about information warfare and, specifically, computer systems being attacked. [The Executive Assistant] recalled that during his CIA tenure, Deutch and he became aware of efforts by [others] to attack computer systems.

98. The computer specialist who provided regular information support to Deutch while he served at DoD, was hired at Deutch's request in June 1995 to provide computer support to the DCI Area. After arriving at CIA, the computer specialist provided direct computer support to Deutch about once per week. At times, Deutch, himself, would directly contact the computer specialist for assistance.

99. The computer specialist described Deutch as a "fairly advanced" computer user who sought and used software that was considered to be above average in complexity. Deutch was further described as having "more than a passing interest in technology" and asking complex computer-related questions. The computer specialist found that Deutch "kept you on your toes"' with questions that required research [for] the answers. Deutch was also described as having a heightened interest in the subject of encryption for computers. The computer specialist recalled that all computer equipment issued to Deutch was appropriately labeled for classified or unclassified work.

100. The computer specialist remembered a conversation with Deutch on the subject of computer operating systems creating temporary documents and files. This conversation occurred while the computer specialist restored information on Deutch's computer after it had failed (i.e., crashed). Deutch watched as documents were recovered and asked how the data could be restored. Deutch was also curious about the utility software that was used to recover the documents. The computer specialist explained to Deutch that data was regularly stored in temporary files and could be recovered. Deutch appeared to be "impressed" with the recovery process.

101. During another discussion, the computer specialist recalled telling Deutch that classified information could not be moved to or processed on an unclassified computer for security reasons.

102. The computer specialist considered Deutch to be a knowledgeable Internet user who had initially utilized this medium while a member of the scientific community at the Massachusetts Institute of Technology. During September 1996 and while Deutch was still serving as DCI, the unclassified CIA Internet web page was altered by a group of Swedish hackers. During discussions with the computer specialist concerning this incident, Deutch acknowledged that the Internet afforded the opportunity for the compromise of information.

103. C/ISMS, who supervised computer support provided to Deutch from the time of his arrival

at CIA through October 1996, considered Deutch to be a computer "super user." Deutch only sought assistance when computer equipment was in need of repair or he desired additional software. The computer support supervisor stated that all unclassified computers and PCMCIA cards that were provided for Deutch's use had green labels indicating they were for unclassified purposes.

104. The LAN technician, who initially configured Deutch's computers at CIA, stated that he labeled all equipment to reflect whether it was designated for classified or unclassified purposes. The technician's stated purpose was to make it clear to Deutch what information could be processed on a particular computer given the requirement that Deutch have access to both classified and unclassified computers.

HAD DEUTCH PREVIOUSLY BEEN FOUND TO HAVE MISHANDLED CLASSIFIED INFORMATION?

105. Beginning in 1977, when he was the Director of Energy Research at the Department of Energy (DoE), Deutch had a series of positions with U.S. Government agencies that required proper handling and safeguarding of classified information to include sensitive compartmented information and DoE restricted data.

106. From 1982 to 1988, Deutch was a paid consultant to the CIA's National Intelligence Council. In 1984, he was also under contract to the CIA's Directorate of Intelligence, Office of Scientific Weapons and Research, serving as a member of the DCI's Nuclear Intelligence Panel.

107. [CIA records reflect Deutch had problems before becoming Director with regard to the handling of classified information. Other specific information on security processing and practices has been deleted due to its level of classification.] Deutch served as DoD's Undersecretary for Acquisitions and Technology and Deputy Secretary of Defense prior to his appointment as DCI.

108. On November 21, 1995, DCI Deutch signed a CIA classified information non-disclosure agreement concerning a sensitive operation. Several provisions pertain to the proper handling of classified information and appear to be relevant to Deutch's practices:

I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, ...

I have been advised that ... negligent handling of classified information by me could cause damage or irreparable injury to the United States ....

I have been advised that any breach of this agreement may result in the termination of any security clearances I hold; removal from any position or special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances ....

I agree that I shall return all classified materials, which have, or may come into my possession or for which I am responsible because of such access ... upon the conclusion of my employment ....

I have read this Agreement carefully and my questions, if any, have been answered.

OIG also obtained similar, non-disclosure agreements signed by Deutch during his employment at DoD.

WHAT LAWS, REGULATIONS, AGREEMENTS, AND POLICIES HAVE POTENTIAL APPLICATION?

109. Title 18 United States Code (U.S.C.) § 793, "Gathering, transmitting or losing defense information" specifies in paragraph (f): *Whoever, being entrusted with or having lawful possession or control of any document,*

writing,...or information, relating to national defense ...through gross negligence permits the same to be removed from its proper place of custody ... shall be fined under this title or imprisoned not more than ten years, or both.

110. Title 18 U.S.C. § 798, "Disclosure of classified information" specifies in part:

Whoever, knowingly and willfully ... uses in any manner prejudicial to the safety or interest of the United States ... any classified information ...obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes ... shall be fined under this title or imprisoned not more than ten years, or both.

111. Title 18 U.S.C. § 1924, "Unauthorized removal and retention of classified documents or material" specifies:

Whoever, being an officer, employee, contractor or consultant of the United States, and, by virtue of his office, employment, position or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $1,000, or imprisoned for not more than one year, or both.

112. The National Security Act of 1947, CIA Act of 1949, and Executive Order (E.O.) 12333 establish the legal duty and responsibility of the DCI, as head of the United States intelligence community and primary advisor to the President and the National Security Council on national foreign intelligence, to protect intelligence sources and methods from unauthorized disclosure.

113. Director of Central Intelligence Directive (DCID) 1/ 16, effective July19, 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," reiterates the statutory authority and responsibilities assigned to the DCI for the protection of intelligence sources and methods in Section 102 of the National Security Act of 1947, E.O.s 12333 and 12356, and National Security Decision Directive 145 and cites these authorities as the basis for the security of classified intelligence, communicated or stored in automated information systems and networks.

114. DCID 1/21, effective July 29, 1994, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) specifies in paragraph 2:

All [Sensitive Compartmented Information] must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets physical security standards imposed by the DCI in the physical security standards manual that supplements this directive.

115. Headquarters Regulation (HR) 10-23, Storage of Classified Information or Materials. Section C (1) specifies:

Individual employees are responsible for securing classified information or material in their possession in designated equipment and areas when not being maintained under immediate personal control in approved work areas.

116. HR 10-24, "Accountability and Handling of Collateral Classified Material," prescribes the policies, procedures, and responsibilities associated with the accountability and handling of collateral classified material. The section concerning individual employee responsibilities states:

Agency personnel are responsible for ensuring that all classified material is handled in a secure manner and that unauthorized persons are not afforded access to such material.

117. HR 10-25, "Accountability and Handling of Classified Material Requiring Special Control," sets forth policy, responsibilities, and procedures that govern the transmission, control, and storage of Restricted Data, treaty organization information, cryptographic materials, and Sensitive Compartmented Information. The section states:

Individuals authorized access to special control materials are responsible for observing the security requirements that govern the transmission, control, and storage of said materials. Further, they are responsible for ensuring that only persons having appropriate clearances or access approvals are permitted access to such materials or to the equipment and facilities in which they are stored.

HOW WAS A SIMILAR CASE HANDLED?

118. In November 1996, a senior CIA official was determined to have routinely authored CIA unique, classified documents on his personal home computer and CIA-issued laptop computer configured for unclassified use. Some of the documents were at the Secret and Top Secret/Codeword level. In addition, the senior Agency official had used both computers to visit Internet sites. In addition, the senior official's family members had access to both computers. However, there was no way to determine if the computer hard drives had been compromised.

119. On December 12, 1996, [the] OPS Legal Advisor, referred a crimes report to the Associate General Counsel (AGC) in the CIA Office of General Counsel. On December 13, 1996, the AGC forwarded to DoJ a crimes report on this incident. In June 1997, a Personnel Evaluation Board (PEB) decided to downgrade the official from an SIS-06 to SIS-05, issue a two-year letter of reprimand including caveats against monetary and non-monetary awards and promotions, and suspend the official for 30 workdays without pay. In addition, the PEB directed the Office of Congressional Affairs to brief the appropriate Congressional intelligence committees about this senior official's breach of security. On September 11, 1997, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were briefed on this incident by Executive Director David Carey.

WHAT ACTIONS DID SENIOR AGENCY OFFICIALS TAKE IN HANDLING THE DEUTCH CASE?

What actions were taken by senior Agency officials after learning of this matter?

120. After learning from O'Neil on December 17, 1996 that classified information had been discovered at Deutch's Maryland residence, Slatkin brought the issue to the attention of Acting DCI George Tenet within one day. She asserted there were multiple discussions with Tenet over time and "everything" had his concurrence. Slatkin explained that the issue was too sensitive for her and Tenet had the responsibility for making the decisions relating to the Deutch incident. Slatkin stated she was also concerned that others may have perceived that she and O'Neil, due to their close association with Deutch, should recuse themselves from the matter. Slatkin said that Tenet gave her the responsibility for coordinating this matter. She relied on O'Neil for legal advice and Calder for a technical review.

121. Calder recalled one or possibly two "late night discussions" with Tenet concerning the Deutch incident. One meeting was to provide Tenet "'the lay of the land." At the second meeting, Tenet gave instructions for the investigation to proceed unimpeded.

122. Tenet stated he first learned of the discovery of classified information on the Maryland computer in December 1996 or January 1997 from either the Chief, DCI Security Staff

or from the C/DCI Administration. Tenet recalled that Slatkin and O'Neil got involved in deciding how to handle the issue. Tenet did not hear about any disagreements concerning the handling of this matter and believed that Slatkin and O'Neil did not want to place Tenet in the position of adjudicating a matter involving Deutch.

123. O'Neil stated that he is uncertain how he first learned of the discovery of classified information on Deutch's Maryland computer. However, according to C/DCI Administration, a meeting was held on the afternoon of December 17, 1996 with O'Neil. At that meeting, O'Neil stated Deutch was concerned about retaining his personal information before returning the four PCMCIA cards to CIA. C/DCI Administration offered a solution by offering to provide Deutch with replacement PCMCIA cards on which Deutch could transfer his personal information. O'Neil passed this suggestion to Deutch, and Deutch agreed. Afterward, the contract network engineer also talked to Deutch about copying his personal information to the new PCMCIA cards. The contract network engineer recalled Deutch wanting to review the files on the original PCMCIA cards because they contained personal information.[17]

124. [The] PDGC learned of the matter on the day of its discovery. Between that date, December 17, 1996, and the date SIB began its investigation, the PDGC recalled there was an ongoing dialogue involving O'Neil, Slatkin, and Calder. The PDGC stated that O'Neil kept her abreast of developments.

125. The former ADDA believes that C/DCI Administration initially apprised her of the discovery on December 26, 1996. Her first concern related to properly securing the classified information at the Deutch residence, which the C/DCI Administration said he would handle. Several days later, [she] learned that the magnetic media at the Maryland residence had been secured, although not as expeditiously as she desired. [She] stated that the PCMCIA cards that had been in Deutch's possession were given to O'Neil.

126. The former ADDA stated that Calder, Slatkin, and O'Neil held a series of meetings to discuss how to handle the incident. She recalled other issues surfacing, such as the resident alien employed as a maid at the Deutch residence; Deutch's personal financial records being maintained on government-owned computers; "disks" Deutch carried in his shirt pocket; and other government-issued unclassified computers at Deutch's Belmont residence, the OEOB, and Headquarters that may contain classified information.

127. D/OPS was first briefed on the case by Calder, who became [his] senior focal point with the former ADDA serving as a back-up. D/OPS never discussed the case directly with either Slatkin or O'Neil. He remembered that the specific permission of Slatkin or O'Neil was needed to involve others in the case. According to D/OPS, the former ADDA believed that Slatkin and O'Neil had as their main concern the fear that sensitive and personal information contained in Deutch's journals would leak. Slatkin stated it was standard operating procedure, when dealing with sensitive investigations or operations, to review requests to involve additional individuals. She claimed it was common practice for her to review such requests with the DCI. She does not recall denying any request to involve others in this case.

128. According to C/SIB, D/OPS asked him to conduct a security investigation to determine: (1) if classified information found on Deutch's government-issued unclassified computer had been compromised, and (2) what conditions would allow a compromise to occur. C/SIB said he was to determine the "who, what, where, when, and why." C/SIB expected "noteworthy" information would be compared to the appropriate DCID security standards and adjudication would be based on SIB's findings. He recalled advising the D/OPS that classified

information on unclassified media could involve a potential violation of federal law.

129. The OPS Legal Advisor wrote in a January 7, 1997 MFR that he attended a meeting the previous day with Calder, D/OPS, C/SIB, and an SIB investigator to discuss the discovery of the classified information on the computer at Deutch's Maryland residence. Among the issues discussed were:

Acknowledgment that because this case involves former DCI Deutch, whatever actions are taken by OPS and other parties will be scrutinized very closely. Therefore, it was stressed by everyone at the meeting that the security investigation of this case must follow the same pattern established in other cases where employees have placed classified information on a computer and possibly exposed that information to access by unauthorized individuals.

130. Calder stated that the OPS Legal Advisor was strident in his concern that Deutch be treated the same as any other Agency employee and senior officials should scrupulously avoid showing special treatment to Deutch. Calder agreed that the investigation should resemble those conducted for similar violations by other Agency personnel. He stated he was concerned that he insulate the OPS/SIB personnel and the C/DCI Administration to ensure that they did not "get ground up."

131. Calder stated that he initially assumed this matter would arise again in the future, possibly with a Congressional committee. Therefore, he insisted that the case be conducted in the same manner as for any CIA employee.

How were the Maryland PCMCIA cards handled?

132. SIB sought to obtain and secure all the government-issued computer equipment and magnetic media that had been provided to Deutch, such as the computers and peripherals that were at both Deutch residences. By early January 1997, all government-issued computer equipment and magnetic media used by Deutch had been turned over to SIB with the exception of the four PCMCIA cards that had been observed by the inspection team on December 17, 1996.

133. O'Neil recalled that a DCI Security officer brought him the four PCMCIA cards from the Maryland residence. O'Neil stated he put the PCMCIA cards in his safe and never opened the envelope that contained them. He said he gave the PCMCIA cards to Calder without argument when asked.

134. Calder recalled that O'Neil told him that Deutch wanted the PCMCIA cards destroyed. Calder advocated the position that the cards should not be tampered with and must be maintained in the event of a future leak investigation. According to Calder, O'Neil and Deutch came to realize the PCMCIA cards could not be summarily destroyed. Calder stated that he went to O'Neil on three or four occasions in an attempt to obtain the four PCMCIA cards, and it took two to three weeks to reach a satisfactory arrangement for O'Neil to surrender them.

135. The PDGC also recalled, "We had to hammer O'Neil to give the [PCMCIA] cards to Security." The PDGC believes Slatkin, whose "loyalty to Deutch was incredible," and Deutch pressured O'Neil not to allow others to have access to the personal information on the cards. The PDGC stated that she, Calder, the OPS Legal Advisor, and C/SIB "pushed the other way" and advocated that O'Neil turn the cards over to Security. C/SIB confirmed the difficulty obtaining the four PCMCIA cards in O'Neil's possession.

136. The former ADDA recalled advising Slatkin that the investigation was dragging on, and that unidentified individuals believed that this was being done purposely in order to "cover up" the event. The former ADDA told Slatkin that O'Neil's withholding of the four cards supported the "cover up" perception.

137. According to Slatkin, after the former ADDA told Slatkin about the problem with the four remaining disks, she requested a meeting with Tenet, O'Neil, and Calder. Tenet reportedly told O'Neil to surrender the PCMCIA cards to Calder. Calder stated that O'Neil claimed that, although Calder had discussed his need for the cards, Calder had never specifically asked O'Neil to turn them over. C/SIB states that Calder, in his presence, "specifically ask[ed]" O'Neil to release the PCMCIA cards. Slatkin said she would have reacted earlier if she had known of Calder's concern.

138. According to O'Neil, he, Tenet, Slatkin, and Calder had conversations over a period of several weeks on the exploitation of the PCMCIA cards and protecting Deutch's privacy. After Tenet decided on the process for handling the cards, they were delivered to Calder. O'Neil said he never refused to turn over the cards for exploitation.

139. O'Neil surrendered the four PCMCIA cards to Calder on February 3, 1997. Calder provided the cards to C/SIB on February 4, 1997.

What was the course of the Special Investigations Branch's investigation of Deutch?

140. Calder stated that, in his view, Slatkin and O'Neil did not want Deutch's name "to be besmirched" and O'Neil assumed the role of an "interlocutor." He also said that Slatkin and O'Neil were particularly sensitive that a possible vendetta would be orchestrated by security personnel as a response to interference by O'Neil and Slatkin in a previous, unrelated, joint investigation involving the DoD.[18] Calder characterized his encounters with Slatkin regarding the Deutch investigation as "always difficult discussions" and that it was continually necessary to "push forward" and achieve "a negotiated peace." Slatkin, however, stated that she had no involvement in the DoD-CIA investigation except to determine why the Acting Director and she had not been informed of the notification to DoD.

141. The OPS Legal Advisor believes Slatkin "constrained the investigative apparatus." He cited, as an example, Slatkin advocating allowing Deutch to go into the files to determine if the information was personal or belonged to the CIA. The OPS Legal Advisor stated that the policy has always been that an individual who places personal information on a government computer loses the expectation of privacy and the material reverts to the control of the government authorities. The OPS Legal Advisor stated that Calder, D/OPS, and the former ADDA tried to keep the investigation on track. Slatkin denied interfering with the investigation. She stated that she did not make any unilateral decisions about the course of the investigation. All requests made by Deutch were relayed to O'Neil, Calder, and Tenet.

142. In the early stages of SIB's investigation, Calder recalled telling Tenet there was no indication of a compromise and the investigation was proceeding. Calder said that the investigators showed him some of the classified material. It included Top Secret/ [Codeword] information; collection methods and imagery; and possibly information identifying CIA operations officers.

143. Calder stated that after a complete package of Deutch's material was recovered from the magnetic media, the question arose as to the proper person to review the material. Because the material contained personal information, Calder recalled that Deutch wanted to review the material himself or have O'Neil do the review. Ultimately, Slatkin selected D/OPS for the task.

144. As part of the SIB investigation, C/SIB interviewed staff from DCI Security and the DCI Information Services Management Staff; he also planned to interview [Deutch's Executive Assistant] and Deutch.[19] On March 24, 1997, Calder informed C/SIB that C/SIB

would not be the one to interview Deutch. (Calder later explained to OIG investigators that a concern existed to have somebody who was politically sensitive question Deutch should such an interview prove necessary.) At Calder's request, SIB composed questions to ask Deutch and, on May 15, 1997, forwarded them to D/OPS for review. However, C/SIB also informed Calder that SIB would not continue their efforts because certain interviewees (i.e., Deutch) were not accessible to SIB. Calder agreed.

145. The OPS Legal Advisor stated that, normally, a case similar to Deutch's would not only be referred to SIB for investigation, but a contemporaneous damage assessment would also be conducted. If the subject was a former employee, typically the subject would be banned from holding a security clearance and future CIA employment.

146. After D/OPS reviewed the 17,000 pages of recovered documents, he prepared a report of his findings and attached a copy of C/SIB's separate, signed report. He recalled receiving a "panicky" call from the former ADDA relaying that Slatkin wanted the report immediately.

147. Calder was familiar with D/OPS's report and stated that it was the lone document that he retained following the conclusion of the investigation. He recalled sending the report to Slatkin and receiving it back with marginal comments, possibly asking if the PCMCIA cards had been destroyed. Slatkin recalled that the draft report was hand-carried to her by Calder. After she read the report, she made written editorial comments requesting clarification and returned the draft report to either Calder or D/OPS. She received the final report, reviewed it, and personally handed it to Tenet. Tenet does not remember ever seeing D/OPS's report, nor does he recall any of the details of the report. He said it is possible that someone told him about the report or showed it to him.

148. A signed copy of the D/OPS report dated July 8, 1997, was recovered from the DDA's Registry. It did not have any notes on the text or attached to the document. No copy was ever recovered from the DCI's Executive Registry, the Executive Director's Office, Calder's personal safe, or anywhere in OGC.

149. There was considerable discussion of what should be done with the magnetic media after its material was catalogued. O'Neil said that Tenet's decision was to retain permanently the PCMCIA cards and a copy of all the classified documents. Calder, however, said there was some disagreement among the parties and the ultimate decision was to destroy the material, including the magnetic media. At the end of the investigation, Calder remembered asking D/OPS what happened to the PCMCIA cards and being told the disks were about to be destroyed or had been destroyed. Nevertheless, Calder said he was not certain the cards were destroyed.

150. After D/OPS sent his report to Calder, the OPS Legal Advisor received an e-mail from the C/ALD stating that the PDGC had spoken to Calder about the SIB investigation of Deutch. Calder reportedly said Deutch would be given a code of conduct briefing in conjunction with Deutch's security briefing as a member of the Proliferation Commission.[20] On August 3, 1997, the OPS Legal Advisor sent the C/ALD an e-mail response expressing concern that no one at DoD or the White House had, so far, been notified about a possible compromise of information. He also raised the issue of Deutch retaining his security clearance. The OPS Legal Advisor wrote:

I remain unpersuaded, however, that the CIA has done everything it can in this case to protect CIA and DOD equities. The investigation has been one in name only .... I'm certainly not persuaded that giving this man a security clearance is in the best interest of the U.S. Government or the President .... I mean, jeez, when was the last time a subject of an investigation was not interviewed because he objected to talking to security officers and the EXDIR, a personal friend, used her position to

short circuit an investigation? Let's be honest with each other, this so-called investigation has been handled in a manner that was more designed not to upset friendships than to protect the interests of the U.S.G.

151. C/SIB had also relayed his concerns about the possible exposure of DoD classified material of ongoing military operations. In his chronology, C/SIB wrote that on March 14, 1997, Calder decided appropriate senior level DoD officials should be briefed on a potential compromise. Calder planned to brief Slatkin of this decision. C/ SIB indicated he again reminded Calder of the need for DoD notification on March 24, 1997. The OIG investigation did not locate any information that such notification occurred until OIG notified DoD on June 17, 1998.

152. As of May 1998, when OIG began its investigation, there was no information in Deutch's official Agency security file concerning the SIB investigation or its findings nor was there any evidence of a security adjudication.

SHOULD A CRIMES REPORT INITIALLY HAVE BEEN FILED ON DEUTCH IN THIS CASE?

153. Title 28 U.S.C. § 535, "Investigation of crimes involving Government officers and employees," requires that

any information, allegation or complaint received in a department or agency of the executive branch of the government relating to violations of Title 18 [U.S. Code] involving Government officers and employees shall be expeditiously reported to the Attorney General.

154. Section 1.7(a) of E.O. 12333, United States Intelligence Activities, requires senior officials of the intelligence community to "report to the Attorney General possible violations of federal criminal laws by employees and [violations] of specified criminal laws by any other person ...."This responsibility is to be carried out "as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned...."

155. Pursuant to Part 1.7(a) of E.O. 12333, the DCI and the Attorney General agreed on crimes reporting procedures for CIA on March 2, 1982. These procedures, which are included as Annex D to HR 7-1, were in effect from that time until August 2, 1995, when they were superseded by new procedures.[21] The new procedures are contained in a document, memorandum of Understanding: Reporting of Information Concerning Federal Crimes," signed by DCI Deutch.

156. According to the Memorandum of Understanding (MOU),

[w]hen the General Counsel has received allegations, complaints, or information (hereinafter allegations) that an employee[22] of the Agency may have violated, may be violating, or may violate a federal criminal statute, that General Counsel should within a reasonable period of time determine whether there is a reasonable basis[23] to believe that a federal crime has been, is being, or will be committed and that it is a crime which, under this memorandum, must be reported.[24]

157. In [the] MFR of the OPS Legal Advisor of January 7, 1997, he wrote that another issue discussed was:

The need to determine whether a crimes report will be required after an assessment of the information stored on the drives and the PCMCIA cards. [18 U.S.C. §§ 1924 and 793(f) were briefly discussed.] The General Counsel will make any determination in that regard.

158. The OPS Legal Advisor stated that he understood that Deutch had placed classified information on unclassified CIA computers that were connected to the Internet, and the classified information only "came out of Deutch's head"

when he composed documents on the computer. The OPS Legal Advisor said he did not know or have any information that Deutch had removed documents from controlled areas containing classified information.[25]

159. The OPS Legal Advisor remembered discussing the issue of the possible criminality of Deutch's actions with the PDGC. His position was more conservative than the PDGC's. She raised the point that, as DCI, Deutch had the legal authority to declassify material under his control. This led to her contention that Deutch could not be prosecuted for a security violation. She reportedly cited an instance when then-DCI William Casey inadvertently divulged classified information in an interview with the media.

160. The OPS Legal Advisor provided handwritten notes from January 6, 1997 about a discussion of a possible crimes report with the PDGC:

Talked to [the PDGC]. She already knew about the Deutch leak. Discussed the 793(f) issue. She concluded years ago that the DCI who has authority to declassify cannot realistically be punished under the statute. I expressed my disbelief in that analysis. Hypo - does that put the DCI beyond espionage statutes? No she says that would be a natl. security call ....Returned briefly to information in play. Discussed how there may have been [non-CIA controlled compartmented program material] on the computer. Doesn't this push 793(f) back into play?

161. In his OIG interview, the OPS Legal Advisor said that DoD material and Top Secret/ [the non-CIA controlled compartmented program] material would not qualify for information a DCI had the authority to declassify. He realized that a referral to the FBI would "technically not" be the same as making a crimes report to DoJ. He stated there was a tendency to discuss some cases with the FBI in order to get their procedural advice.

162. The OPS Legal Advisor had a discussion with an FBI agent then assigned to the Counterespionage Group, Counterintelligence Center (CIC), regarding the possible applicability of Title 18 U.S.C. §§ 793(f) and 1924 in the matter regarding Deutch. The OPS Legal Advisor recalled this FBI Agent believing that there had to be a physical removal of documents to constitute a violation of the statutes.

163. A two-page handwritten note of January 24, 1997, composed by the OPS Legal Advisor, reported his discussion with the FBI Agent regarding the case. The note indicated that the FBI Agent at CIC suggested that it was better to have O'Neil call the then-FBI General Counsel discuss the case.

164. The OPS Legal Advisor provided an MFR reporting a January 28, 1997 meeting with the PDGC and O'Neil to discuss the Deutch case. At that time, O'Neil indicated he anticipated calling the FBI General Counsel to tell him CIA intended to conduct an investigation of this matter unless the FBI General Counsel wanted the FBI to assert investigative authority.

165. According to O'Neil, neither he nor anyone else suggested a crimes report be filed on the Deutch matter. O'Neil said a crimes report can be made at several points during an investigation. He pointed out that, in a number of cases, CIA conducts its own investigation. Matters could also be referred to DoJ to conduct an investigation.

166. O'Neil is not certain whether he talked to the FBI agent at CIC about the Deutch matter. O'Neil has a vague recollection he called the FBI General Counsel and asked him how CIA should proceed. O'Neil described the case to the FBI General Counsel, who said that the CIA should continue its own process of looking at the matter. O'Neil believes he wrote an MFR documenting his conversation and may have given the MFR to his secretary to keep in a personal folder used for sensitive matters.[26]

167. The FBI Agent at CIC recalled that he was told Deutch had classified information on a computer disk at his home in Maryland shortly after the matter was discovered. The FBI Agent was asked if the matter was an "811" violation.[27] The FBI Agent concluded there was no reason to believe that the information had been compromised to a foreign power and, therefore, the FBI did not need to get involved. The FBI Agent recalled telling someone at CIA, whose identity he does not remember, that since Deutch was involved, O'Neil may want to contact the FBI General Counsel, O'Neil's counterpart at FBI. The FBI Agent said that he established early on in his tenure at CIA that merely telling him something did not constitute official notification of the FBI much less DoJ. He was aware that OGC had crimes reporting responsibilities, and he expected them to fulfill those responsibilities.

168. The FBI General Counsel recalled a single telephone call from O'Neil after Deutch left CIA, between February and April 1997. At that time, O'Neil told the FBI General Counsel an issue had arisen about classified information existing on some computer disks at Deutch's home. The FBI General Counsel recalled they discussed CIA reporting requirements to the FBI under "811." [He] believes he would have told O'Neil that not enough was known about the matter at the time. If an "811" problem surfaced after CIA had looked into the matter, CIA should refer the problem to the FBI through official CIA channels.

169. The FBI General Counsel stated that he did not consider O'Neil's call as a submission of a crimes report because, from what he remembers being told, there was no evidence of a crime. He said that he and O'Neil spoke on the telephone several times a week, but O'Neil never made a crimes report to him. [He] said that if he thought O'Neil was giving him a crimes report, he would have told him to do it through the proper channel.

170. Calder said that if a referral should have been made to DoJ and was not, he believes the omission was not intentional. However, Calder stated the responsibility for a crimes report was O'Neil's. Calder added that "I have never issued a crimes report and would always raise such an issue with OGC for their action." Calder said the FBI General Counsel had informed O'Neil that DoJ would not pursue a Deutch investigation regarding misuse of the computer.

171. The PDGC had supervisory responsibility of the Litigation Division, which had the crimes reporting account in OGC at that time.[28] The PDGC stated she did not have a lot of hands-on experience with the mechanics of coordinating crimes reports and had never authored a crimes report. She first learned of the discovery of classified information, including Top Secret/[a non-CIA controlled compartmented program] material, on a computer in Deutch's Maryland residence on the day of its discovery in December 1996. She remembered hearing about information regarding a covert action with [two countries] but does not recall hearing there was [codeword] or [a different codeword] information on the computer. She did not learn that the computer at his Belmont residence also contained classified information.

172. The PDGC was not aware that Deutch was deleting files from the Maryland computer in the days immediately following the discovery of the classified information. She remembered speaking with Calder about the necessity of protecting the magnetic media. Her reason for wanting to retain the magnetic media was not for evidence of a crime but to have a record should there be a need to conduct a leak investigation in the future.

173. When considering the need for a crimes report, the PDGC said she did not examine the "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes." She did not consult with any attorneys from the Internal Security Section of DoJ of with

the United States Attorneys Office. She does not remember reviewing Title 18 U.S.C. § 793(f), "Gathering, transmitting or losing defense information." She spoke with O'Neil's Executive Assistant[29] regarding the provisions of Title 18 and with the OPS Legal Advisor. She did not agree with the OPS Legal Advisor's assertion that, because the classified information "was [only] in his [Deutch's] head," Deutch did not remove classified information from the Agency. The PDGC was aware that, on occasion, Deutch carried the PCMCIA cards "back and forth" with him. She did not know if the cards contained classified information. The PDGC saw no distinction between classified information on a document as opposed to being on magnetic media. She explained that she was more concerned at this time with protecting and recovering the magnetic media than considering a crimes report.

174. The PDGC reviewed the statutes she thought would be relevant and did not see all the elements present for a violation. She believed that Deutch, as DCI, was the authority for the rules concerning the handling of classified information. Because Deutch issued DCIDs on classified material, she believed he could waive the rules for himself. The PDGC recognized that the DCI cannot declassify Top Secret/ [the non-CIA controlled compartmented program] material, but said such material may be handled under the DCID rules. The PDGC stated that given the fact that this matter involved a former DCI, if she had believed a crimes report was necessary, she would have shown the draft to O'Neil and he would have had the final say as to whether a crimes report was warranted.

175. The PDGC focused on Title 18 U.S.C. §1924,"Unauthorized Removal and Retention of Classified Documents or Material." She understood that Deutch was authorized to remove classified information and take it home since he had a safe at his residence. She stated that she did not see "intent"[30] by Deutch. She reasoned that "intent" was a necessary element, "otherwise everyone [inadvertently] carrying classified information out of a CIA building would be the subject of a crimes report." According to the PDGC, Deutch had permission to take the classified material home, and Deutch's use of the PCMCIA cards was permissible within his residence. In the PDGC's view, the security violation occurred when he "did not do it right" by connecting the Internet to his computer and "leaving the card in the slot." She did not distinguish between Deutch as DCI and his actual status as an Independent Contractor when the classified information was discovered. However, she would have looked at the issue differently if she understood that the only acceptable means of safeguarding the computer would have been to remove and secure the computer's hard drive.

176. The PDGC did not remember when she made the legal decision that a crimes report was not required. She remembered speaking with C/SIB in March 1997 about his concern that a crimes report should be filed.

177. The PDGC said that D/OPS's report was not made available to her. Although someone in OGC would usually read OPS reports, the PDGC speculated that the D/OPS would not have shown the report to her without receiving authorization. She never thought to request a copy of the D/OPS's report to determine if his findings were consistent with her decision not to file a crimes report. Later, after she became Acting General Counsel, the issue of her reviewing the report never arose, and she would have expected OPS to raise the report with her only if the facts had changed significantly from what she learned initially.

178. In comparing the Deutch case to a similar case involving a senior Agency official, the PDGC asserted that the other official did not have a safe in his residence and was not authorized to take home classified information. She viewed this dissimilarity as a major distinction. Nor did he have the authority to waive the rules on the handling of classified information. The PDGC did not remember

if OGC made a crimes report on that case of mishandling classified information.[31]

179. George Tenet, who was Acting DCI at the time of the OPS/SIB investigation, said no one ever raised the issue of reporting this incident to DoJ, and it did not occur to him to do so. Tenet said no one ever came forward with a legal judgment that what had occurred was a crime. In Tenet's opinion, based upon what he knew at that time, there was no intent on Deutch's part to compromise classified information. Therefore, Tenet did not believe a crime was committed. Tenet was aware of the incident involving [another] senior Agency official but was not aware a crimes report had been filed on it.

SHOULD APPLICATION OF THE INDEPENDENT COUNSEL STATUTE HAVE BEEN CONSIDERED?

180. The fundamental purpose of the Independent Counsel statute is to ensure that serious allegations of unlawful conduct by certain federal executive officials are subject to review by counsel independent of any incumbent administration.

181. Title 28 U.S.C. § 592, "Preliminary investigation and application for appointment of an independent counsel" cites Title 28 U.S.C. § 591, "Applicability of provisions of this chapter," as the basis for those positions who are "covered persons" under the Independent Counsel statute.

182. Title 28 U.S.C. § 591 (a), "Preliminary investigations with respect to certain covered persons," specifies:

The Attorney General shall conduct a preliminary investigation in accordance with Section 592 whenever the Attorney General receives information sufficient to constitute grounds to investigate whether any person described in subsection (b) may have violated any Federal criminal law other than a violation classified as a Class B or C misdemeanor or an infraction.[32]

183. Title 28 U.S.C. § 591 (b), "Persons to whom subsection (a) applies" lists:

... the Director of Central Intelligence [and] the Deputy Director of Central Intelligence....[33]

184. Title 28 U.S.C. § 591 (d) (1), "'Examination of information to determine need for preliminary investigation," "factors to be considered" specifies:

In determining ... whether grounds to investigate exist, the Attorney General shall consider only -- (A) the specificity of the information received; and (B) the credibility of the source of the information.

185. The Deputy Chief, Public Integrity Section, Criminal Division, DoJ, is responsible for the preliminary review of matters referred to DoJ under the provisions of the Independent Counsel statute. [She] explained that the provisions of the Independent Counsel statute require DoJ to review an allegation regarding a "covered person" to determine the need for preliminary investigation based only on the two factors listed above.

186. The Deputy Chief of the Public Integrity Section explained that after the CIA IG referral in March 1998, the Public Integrity Section reviewed the matter and described it in a memorandum to the Attorney General. The memorandum stated that the allegations of illegal behavior regarding former DCI Deutch were received more than one year after Deutch left office. Accordingly, under the provisions of the Independent Counsel statute, Deutch was no longer a "covered person." The Deputy Chief of the Public Integrity Section added that the allegation should have been promptly referred to DoJ by CIA personnel.

187. The OPS Legal Advisor stated that he never considered the need to refer this matter to an Independent Counsel based on Deutch's status as a "'covered person." Nor was he aware of any other discussions on this matter.

188. The PDGC stated that the issue of Deutch being a "covered person" under the Independent Counsel legislation did not arise. She said that "she never gave a thought," to the applicability of the Independent Counsel statute, and she does not know what positions within the Agency are specified as "covered persons."

189. O'Neil stated that there was no recommendation to refer the Deutch matter to DoJ under the provisions of the Independent Counsel statute.

WERE SENIOR AGENCY OFFICIALS OBLIGATED TO NOTIFY THE CONGRESSIONAL OVERSIGHT COMMITTEES OR THE INTELLIGENCE OVERSIGHT BOARD OF THE PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD? WERE THESE ENTITIES NOTIFIED?

190. Pursuant to the National Security Act of 1947, as amended, the President and the DCI bear statutory responsibility for keeping the two Congressional intelligence committees fully and currently informed of all intelligence activities.

191. Agency Regulation (AR) 7-2, "Reporting of Intelligence Activities to Congress," provides interpretation of the statutes so the Agency, with the assistance of the Office of Congressional Affairs and the Office of General Counsel, can assist the DCI in meeting the obligation to keep the intelligence committees fully and currently informed. Under the section, "Obligation to Keep Congressional Intelligence Committees Fully and Currently Informed," one of the three categories requiring reporting are:

Particular intelligence activities or categories of activities as to which either of the Congressional intelligence committees has expressed a continuing interest (for example, potentially serious violations of U.S. criminal law by Agency employees, sources, or contacts);

192. E.O. 12863, issued September 13, 1993, President's Foreign Intelligence Advisory Board, specifies:

The heads of departments and agencies of the Intelligence Community, to the extent permitted by law, shall provide the Intelligence Oversight Board (IOB)[34] *with all information that the IOB deems necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community, to the extent permitted by law, shall report to the IOB, at least on a quarterly basis and from time to time as necessary or appropriate, concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.*

193. According to the Director of the CIA's Office of Congressional Affairs (OCA), OCA is responsible for notifications to Congress and should be informed of any formal Agency investigations. OCA receives notifications from a variety of Agency components. During Slatkin's tenure, all formal written Congressional notifications were to be routed through her office. The Director of OCA was unaware of SIB's investigation into the discovery of classified information on Deutch's government-issued unclassified computer.

194. At the January 6, 1997 meeting to discuss the planned investigation of the finding of classified information on Deutch's unclassified CIA computer, the OPS Legal Advisor stated that the Congressional oversight committees may eventually inquire about this matter. He recalled that Calder wanted the investigation performed "by the book" in case there would be a need to account for SIB actions.

195. Calder assumed this matter would again arise in the future, possibly through a leak,

with a Congressional committee. He recalled a discussion about doing briefings and was left with the impression that there was a briefing of the "Group of Four" Congressional oversight committees.[35]

196. C/SIB maintained a chronology of the investigation consistent with Calder's instructions. He also advised Calder, the former ADDA, the PDGC, and the D/OPS on at least two occasions that Congress, along with DoD, should be informed about the material found on Deutch's unclassified computer. After receiving a copy of the D/OPS's report on the investigation, C/SIB realized the report did not contain a recommendation that Congress be notified.

197. The PDGC stated she did not remember any discussion concerning notifying the Congressional oversight committees or the IOB. O'Neil said that "the question of informing the IOB or the Congressional oversight committees did not come up."

198. Slatkin stated she could not recall any discussion or recommendation regarding the need to notify the Congressional committees about the Deutch matter. In her interview with OIG, she stated that, "surely, yes, the Committees should have been notified--but at what point?"

199. The IOB was officially notified of OIG's investigation on May 8, 1998. After being informed of the OIG investigation, the Director of Congressional Affairs prepared talking points, which DCI Tenet presented to the SSCI and HPSC1 in early June 1998.

WHY WAS NO ADMINISTRATIVE SANCTION IMPOSED ON DEUTCH?

200. Deutch was aware that an inquiry was conducted after classified information was discovered on his government-issued computers configured for unclassified use. He said that he never tried to influence the outcome of the investigation. Nor was he told the outcome, although he had requested that someone apprise him of the results.

201. Calder said that, despite the pressure that accompanied the investigation of a DCI, he and OPS did "the right thing." Calder said that since Deutch was no longer a CIA employee, there was no punishment that could be administered to him. The issue was what position the Agency should take if Deutch needed access to classified information in the future. Calder was aware that Deutch's computers had been replaced with totally unclassified magnetic media. Calder said that while Deutch was on several governmental committees, he did not believe that Deutch had a need for classified information in those positions. Calder said the remedy was to counsel Deutch in a discrete manner that would not offend his ego so he would understand the gravity of what had happened. Calder was aware that Slatkin had spoken with Deutch about the issue, and, from those conversations, Deutch would have recognized that his actions were wrong. Calder stated it was his responsibility to counsel Deutch and he planned to do so when Deutch received a briefing regarding future access. However, Calder said he never had the opportunity to meet with Deutch under the conditions he desired.

202. The former ADDA stated that she was "worn down" by Slatkin and O'Neil, and perceived that the D/OPS and Calder were similarly affected. Additionally, Calder was "frustrated" because Slatkin would not resolve issues presented to her but, instead, provided more tasking. The former ADDA said that she, the D/OPS, and Calder had reached a point where they could not go any further in that there was no additional merit in further evaluating the collected data. Slatkin had "emotional attachments" and O'Neil was not considered to be objective. According to the former ADDA, Slatkin's and O'Neil's oversight of the investigation was colored by a distrust of OPS and an interest to protect Deutch's privacy. The former ADDA said that she and SIB

investigators perceived Slatkin's and O'Neil's behavior as "stonewalling." The former ADDA and SIB investigators also viewed Slatkin's requests for repeated clarifications, while typical of her management style, as a form of "pressure" to wear down the others until they were ultimately in agreement with her and O'Neil.

203. The PDGC said that there was not a "crisp end" to the case; "it ran out of steam" when many of the principals left the Agency. The PDGC thought a decision was made that the Director of the Center for CIA Security or the D/OPS would brief either Deutch or the whole Proliferation Commission regarding safeguarding classified information, but she does not know if this action was taken. O'Neil stated that after the process for producing the review was approved by the ADCI, who had been kept informed all long, he had little to do with the investigation. O'Neil also stated, he did not interfere with the OPS investigation, he left the Agency in July 1997,[36] and he does not know how the investigation was concluded. Slatkin said that she gave the information to Tenet and assumed that the investigation would have proceeded after she departed the Agency. The D/OPS said that, as far as he knows, no decision was ever made on what to do concerning Deutch's actions.

204. Tenet did not recall how the matter was resolved. He believes Calder, the D/OPS, Slatkin, and O'Neil had detailed discussions on the matter. Tenet was aware of concerns for Deutch's privacy. According to Tenet no one ever raised the issue of reporting the incident to the Department of Justice, or whether Deutch's clearance should be affected.

WHAT WAS OIG'S INVOLVEMENT IN THIS CASE?

When did OIG first learn of this incident?

205. The former C/DCI Administration spoke with then-IG Frederick Hitz on December 18, 1996[37] regarding what was found at Deutch's residence. The former C/DCI Administration described conversations he had with O'Neil and Slatkin about the matter, and O'Neil's assertion that the former C/DCI Administration was responsible for allowing Deutch to improperly process classified information. Hitz instructed the former C/DCI Administration to provide the IG with copies of any documentation,[38] encouraged the former C/DCI Administration to brief Tenet as soon as possible, and suggested that the former C/DCI Administration stay in contact with the IG.

206. According to the former C/DCI Administration's MFR of December 30, 1996, the IG Counsel contacted him on December 19, 1996. Reportedly, the IG Counsel urged the former C/DCI Administration to prepare an MFR and provide related documentation to the IG.

207. On December 20, 1996, Hitz called the former C/DCI Administration to inform him that he had met with Tenet, who was reportedly not aware of the Deutch matter. Hitz indicated that he and Tenet both supported the process that was being pursued on the acquisition of relevant information and the classified magnetic media. Hitz encouraged the former C/DCI Administration to ensure that his documentation was forwarded to Hitz's staff for the former C/DCI Administration's protection.

208. Hitz remembers that in mid-December 1996, the former C/DCI Administration met with him regarding classified information discovered on one or two Agency-owned computers at Deutch's residences in Maryland and Belmont. Hitz recalled the former C/DCI Administration seeking advice on what action to take. Hitz's impression was that C/DCI Administration was concerned that the former C/DCI Administration's supervisors would not act appropriately. Hitz understood that the classified information found on Deutch's computer included sensitive trip reports. The computer was connected to the Internet, and

there was [a] threat of the information being vulnerable to electronic compromise.

209. Hitz believes that he discussed the former C/DCI Administration's information with IG Counsel and the then-Deputy IG for Investigations and obtained their advice. This advice included instructing the former C/DCI Administration to secure the hard drive and other classified information that was recovered from Deutch's computers. Hitz remembered passing that instruction to the former C/DCI Administration. Hitz recalled that after meeting with IG Counsel and then-Deputy IG for Investigations, "'we knew we were going to get into it and be helpful with it."

210. Hitz stated that he cannot remember what follow-up instruction he may have provided to IG Counsel and then-Deputy IG for Investigations. Hitz thinks he ultimately read the former C/DCI Administration's MFR and "did not like the smell of it" [the nature of the allegation] and "if half of what the former C/DCI Administration said was true - we would get in it." Hitz emphasized that the determination of whether to get involved would be made in concert with IG Counsel and the then-Deputy IG for Investigations. Hitz stated he never discussed the SIB investigation with Deutch, Slatkin, O'Neil, Calder, the PDGC, or D/OPS.

211. IG Counsel said that he does not remember any discussions that Hitz may have had with him and the then Deputy IG for Investigations stemming from information received from the former C/DCI Administration. The IG Counsel stated that he does not remember calling the former C/DCI Administration or having any discussion of an allegation regarding Deutch, nor does he remember seeing an MFR by the former C/DCI Administration.[39]

212. The then-Deputy IG for Investigations said there were contacts between the former C/DCI Administration and Hitz over this issue, and Hitz would tell the then-Deputy IG for Investigations about the conversations afterwards. The then-Deputy IG for Investigations stated he "may have detected an inference from Hitz that classified information was on the computer." However, the then-Deputy IG for Investigations did not remember any discussion with Hitz regarding the need to protect the computer's hard drive. The then-Deputy IG for Investigations was not in contact with the former C/DCI Administration.

Why did OIG wait until March 1998 to open an investigation?

213. Hitz observed that the investigation had started with the former C/DCI Administration's "security people" finding the data, and the investigation stayed in a security channel. Hitz believed that it was appropriate for that to continue as long as OPS would be allowed to do their job.

214. C/SIB's chronology noted a call from the then-Deputy IG for Investigations on January 7, 1997 asking that SIB look at a particular issue, normally the purview of the OIG (improper personal use of a government computer) to put some preliminary perspective to the issue and keep him apprised.

215. The then-Deputy IG for Investigations stated that he must have learned from Hitz that C/SIB was involved with an investigation related to Deutch and that knowledge prompted the then-Deputy IG for Investigations to call C/SIB on January 7, 1997. The then-Deputy IG for Investigations said that, if he had been informed that the matter under investigation by C/SIB was a "serious issue," he would remember it. The then-Deputy IG for Investigations categorized the issue under investigation by SIB as one of "propriety and property management." He does not recall knowing that the computers involved were intended for unclassified use.

216. The OPS Legal Advisor stated he learned

from Calder that on January 5, 1997, Hitz was briefed on the incident involving Deutch. Reportedly, Calder stated that Hitz believed that the incident was a security issue and not one for the IG. After learning of Deutch's possible appointment to the Office of Science and Technology Policy, on May 16, 1997, [the OPS Legal Advisor] wrote in an MFR that he met briefly with Hitz to discuss Deutch's possible appointment and

Fred [Hitz] said he would speak to the DCI about this matter, and sensitize him to the problems associated with [Deutch's] needing a clearance at another U.S.G. agency. Fred asked to be kept informed.[40]

217. According to C/SIB, he contacted OIG to define OIG interests before the D/OPS began his review of the recovered documents. C/SIB met with the then-Deputy IG for Investigations, the IG Counsel, and the then-Deputy Associate IG for Investigations. C/SIB advised them that any difficulties he encountered to date were within his ability to resolve. In his chronology, C/SIB writes:

C/SIB met with [the then-Deputy IG for Investigations, the Deputy Associate IG for Investigations and the IG Counsel] re "reporting threshold" to OIG for USG Computer Misuse, both in this case in particular, and in other cases, in general. This meeting was imperative in order for C/SIB to know before the "security" review [being conducted by [the] D/OPS] what would vice would not be OIG reportable. Upon discussion, it was determined that the OIG would avail great latitude to SIB re such reporting, noting that only in instances wherein the use of the computer was obviously criminal in nature, a conflict of interests [sic] existed, an outside business was being conducted, or a private billing reimbursement for "personal entertainment" was in evidence, would the OIG require a report be submitted by SIB. (C/SIB so advised D/OPS). No particulars[41] *were discussed relative to SIB's ongoing investigation, nor were any requested.*

218. The then-Deputy IG for Investigations remembers the February 21, 1997 meeting with C/SIB in the presence of the Deputy Associate IG for Investigations, and possibly the IG Counsel. Up to that point, OIG had lost track of the allegation against Deutch. The then-Deputy IG for Investigations stated he told C/SIB about OIG's jurisdictional interests in terms of the computer. The then-Deputy IG for Investigations said it is possible that C/SIB made some comment about encountering some difficulty in the investigation but was working through the problem and appeared self-confident about his capability to investigate the matter. The then-Deputy IG for Investigations sensed that C/SIB was being "squeezed by unspecified OPS officials."

219. The then-Deputy IG for Investigations remembered C/SIB agreeing that he should re-contact OIG if he encountered any matter of IG interest, such as evidence of misuse of an official computer, during his investigation. According to the then-Deputy IG for Investigations, "there was no zest" on the part of OIG to take it over while OPS was working the issue. The then-Deputy IG for Investigations does not recall knowing at the time that the OPS/SIB investigation involved classified information.

220. On February 6, 1998, the Deputy Associate IG for Investigations met with C/SIB on an unrelated investigation. C/SIB incorrectly assumed the Deputy Associate IG for Investigations was investigating Deutch's mishandling of classified information on a computer at his residence. According to the Deputy Associate IG for Investigations, C/SIB disclosed that he was unable to fully pursue his investigation because of a problem with Slatkin and O'Neil. C/SIB was frustrated because there had been no interview of Deutch, a customary part of an SIB investigation.

221. During this meeting, the Deputy Associate

IG for Investigations reviewed a number of documents that included an unsigned report prepared by the D/OPS. This report detailed the D/OPS review of data discovered on the Deutch's magnetic media. The Deputy Associate IG for Investigations, subsequently met with the then-Deputy IG for Investigations, and told him what he had learned from C/SIB.

222. In his OIG interview, the then-Deputy IG for Investigations explained that OIG opened an investigation because SIB's investigation was impeded or "shutdown," and a crimes report was never sent to DoJ.

223. Hitz explained that a security violation of this nature would not normally be a matter investigated by OIG.[42] He stated that as the IG, he would have been inclined to assert investigative authority only when he believed that the normal management response was inappropriate or not helpful. He recognized that Deutch appointees Slatkin and O'Neil were involved in the review process. Hitz stated that it was the responsibility of OIG "to support the institution."

What steps were taken by OIG after opening its investigation?

224. IG Counsel remembered advising the Deputy Associate IG for Investigations that the allegation had to be referred to DoJ as a possible crimes report. The IG Counsel also remembers a discussion about the relevance of the Independent Counsel statute since Deutch was a "covered person."

225. On March 19, 1998, OIG referred the allegations to DoJ. The crimes report letter noted that at the time of the alleged violations, Deutch was a "covered person" under the Independent Counsel statute. DoJ advised they would review the allegations for applicability to the Independent Counsel statute and further OIG investigation was not authorized until completion of DoJ's review. In May 1998, DoJ informed OIG that the Independent Counsel statute would not apply because DoJ was not notified of the alleged violations until more than one year after Deutch left his position. As such, Deutch's status as a "covered person" had expired.

226. On May 8, 1998, OIG informed the Chairman of the Intelligence Oversight Board by letter of the criminal investigation of Deutch pursuant to E.O. 12863.

227. On June 2 and 3, 1998, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence were notified by DCI Tenet that the OIG was conducting an investigation of former DCI Deutch and the manner in which the matter was originally handled by CIA officials.

WHAT IS DEUTCH'S CURRENT STATUS WITH THE CIA?

228. Deutch's no-fee, December 1996 consulting contract was renewed in January 1998 and December 1998. The latest renewal covers the period December 16, 1998 until December 15,1999. This contract provides Deutch with staff-like access to the Agency, its computer system, and a Top Secret clearance. Deutch's contract for the Proliferation Commission will expire when the commission finishes its work. That contract does not contain any information regarding access to classified information.

WHAT WAS THE DISPOSITION OF OIG'S CRIMES REPORT TO THE DEPARTMENT OF JUSTICE?

229. On April 14, 1999, Attorney General Janet Reno sent a letter to DCI Tenet [declining prosecution.] [The letter stated in part:]

The results of that [OIG] investigation have been reviewed for prosecutive merit and that prosecution has been declined. As I understand that Mr. Deutch currently holds a Top Secret security clearance, I suggest that the appropriate security officials at the

Central Intelligence Agency review the results of this investigation to determine Mr. Deutch's continued suitability for access to national security information.

CONCLUSIONS

230. Former DCI John Deutch was specifically informed that he was not authorized to process classified information on government computers configured for unclassified use.

231. Throughout his tenure as DCI, Deutch intentionally processed on those computers large volumes of highly classified information to include Top Secret Codeword material.

232. Because Deutch's computers configured for unclassified use had connections to the Internet, all classified information on those computers was at risk of compromise. Whether any of the information was stolen or compromised remains unknown.

233. On August 1, 1995, Deutch was made aware that computers with Internet connectivity were vulnerable to attack. Despite this knowledge, Deutch continued his practice of processing highly classified material on unclassified computers connected to the Internet.

234. Information developed during this investigation supports the conclusion that Deutch knew classified information remained on the hard drives of his computers even after he saved text to external storage devices and deleted the information.

235. Deutch misused U.S. Government computers by making extensive personal use of them. Further, he took no steps to restrict unauthorized persons from using government computers located at his residences.

236. The normal process for determining Deutch's continued suitability for access to classified information, to include placing the results of the SIB investigation in Deutch's security file, was not followed in this case, and no alternative process was utilized. The standards that the Agency applies to other employees' and contractors' ability to access classified information were not applied in this case.

237. Because there was a reasonable basis to believe that Deutch's mishandling of classified information violated the standards prescribed by the applicable crimes reporting statute, Executive Order and Memorandum of Understanding, OGC officials Michael O'Neil and the PDGC should have submitted a crimes report to the Department of Justice.

238. The actions of former Executive Director Nora Slatkin and former General Counsel Michael O'Neil had the effect of delaying a prompt and thorough investigation of this matter.

239. DDA Richard Calder should have ensured the completion of a more thorough investigation, in particular, by arranging for an interview of Deutch and a subsequent documentation of that interview in accordance with established Agency procedures. Calder should also have ensured that the matter was brought to a conclusion rather than permitting it to languish unresolved.

240. Former Inspector General Frederick Hitz should have involved himself more forcefully to ascertain whether the Deutch matter raised issues for the Office of the Inspector General as well as to ensure the timely and definitive resolution of the matter.

241. DCI George Tenet should have involved himself more forcefully to ensure a proper resolution of this matter.

242. The application of the Independent Counsel statute was not adequately considered by CIA officials and, given the failure to report to DoJ on a timely basis, this in effect avoided the potential application of the statute.

243. The Congressional oversight committees and the Intelligence Oversight Board should have

been promptly notified of Deutch's improper handling of classified information.

Daniel S. Seikaly

RECOMMENDATIONS

1. John Deutch's continued suitability for access to classified information should be reviewed immediately.

2. The accountability of current and former Agency officials, including Deutch, for their actions and performance in connection with this matter should be determined by an appropriate panel.

3. All appropriate Agency and Intelligence Community components should be informed in writing of the sensitive information Deutch stored in his unclassified computers so that responsible authorities can take any actions that would minimize damage from possible compromise of those materials.

Aftermath of the IG Report

When the above IG report leaked to the press, it caused such consternation on Capital Hill. 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, Deutch, O'Neil, Slatkin, Executive Director David Carey, and DCI Tenet. O'Neil exercised his Fifth Amendment right not to testify before the Committee. In addition, former Senator Rudman, PFIAB Chairman, briefed the SSCI on the findings of the Board's report on the Deutch matter.
The Committee confirmed that Deutch's unclassified computers contained summaries of sensitive US policy discussions, references to numerous classified intelligence relationships with foreign entities, highly classified memorandums to the President, and documents imported from classified systems. As the DCI, 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, the SSCI determined that he failed in this responsibility. 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 believed further that, in their response to 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. The committees were not notified of the security breach by Deutch until more than 18 months after its discovery.

The Committee determined that there were gaps in existing law that required legislative action. The 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 CIA Act of 1949 to broaden the notification requirement. The new notification requirements include former DCIs, 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: (1) review Deutch's continued

access to classified information, (2) establish a panel to determine the accountability of current and former CIA officials with regard to the Deutch matter, (3) and advise appropriate CIA and Intelligence Community components of the sensitive information Deutch stored on his unclassified computers. DCI Tenet responded to the IG report by indefinitely suspending 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 PFIAB 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 the 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.

After CIA Director Tenet revoked Deutch's intelligence clearances, the Department of Justice reconsidered its initial decision made in April 2000 not to prosecute Deutch. After another review, Justice decided to go forward with a prosecution. Before any trial began, Deutch and Justice reached a plea agreement, but it was short-circuited when President Clinton pardoned Deutch in January 2001.

Endnotes

[1] OPS was established in 1994 and was submitted as part of the new Center for CIA Security in 1998. The mission of OPS was to collect and analyze data on individuals employed by or affiliated with the Agency for the purpose of determining initial and continued reliability and suitability for access to national security information. SIB conducts investigations primarily related to suitability and internal security concerns of the Agency. SIB often works with OIG, handling initial investigations, and refers cases to the OIG and/or proper law enforcement authority once criminal conduct is detected.

[2] Congressional oversight is provided by the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). The two appropriations committees—the Senate Appropriations Committee, Subcommittee on Defense (SAC) and the House Appropriations Committee, National Security Subcommittee (HAC)—also bear oversight responsibilities.

[3] Hereafter, the residences will be referred to as Maryland and Belmont.

[4] This division has since been renamed the Administrative Law and Ethics Division.

[5] According to his July 14, 1998 OIG interview, C/ALD prepared the MFR, and it was cosigned by the PDGC and (him). (He) stated that he took the only copy of it, sealed it in an envelope, and retained it. He sensed that it was likely there would eventually be an Inspector General investigation of the computer loan. (He) stated that this was the only time in his career that he has resorted to preparing such an MFR. He stated that he did not tell O'Neil about the MFR nor provide a copy to O'Neil since he judged that to be "unwise." He did not provide a copy of it to the OGC Registry. He said that he has kept it in his "hold box" since he wrote it.

[6] The OIG investigation has not located any contract that includes a third computer.

[7] The Infosec Officer did not copy the sixth document, a letter to DCI nominee Anthony Lake that contained Deutch's personal sentiments about senior Agency officials.

[8] The former ADDA retired in October 1997.

[9] Formatting prepares magnetic media for the storing and retrieval of information. Reformatting eases the tables that keep track of file locations but not the data itself, which may be recoverable.

[10] OIG was unable to determine how the Belmont computer was marked because the chassis was disposed of prior to the OIG investigation.
[11] In response to an authorization for disclosure signed by Deutch, (the ISP) provided business records to OIG. These records reflect that Deutch, using the screen name (that was a variation of his name), maintained an account with (the ISP) since January 1, 1995.
[12] The Department of Defense recovered and produced in excess of 80 unclassified electronic message exchanges involving Deutch from May 1995 through January 1996. These messages reflect Deutch's electronic mail address as (variations of his name).
[13] Certain material viewed by the exploitation team was described as leaving the user's computer particularly vulnerable to exploitation. The exploitation team did not recover this material and it was never viewed by OIG.
[14] Journals containing classified material classified up to TS/SCI encompassing Deutch's DoD and CIA activities were recovered from multiple PCMCIA cards. Deutch stated that he believed his journals to be unclassified.
[15] A "cookie" is a method by which commercial Web sites develop a profile of potential consumers by inserting data on the user's hard drive.
[16] After reading the draft ROI, Deutch's refreshed recollection is that it was in December 1996, not December 1997, that he first became aware that his computer priorities resulted in vulnerability to electronic attack.
[17] In his interview with OIG, Deutch confirmed he reviewed the original PCMCIA cards to delete personal information.
[18] Based on a series of intelligence leaks in the *Washington Times*, CIA's Special Investigations Branch determined that leaks were related to the distribution of intelligence reports at the Pentagon. In a routine procedure, CIA sent a letter to DoD and the Defense Intelligence Agency (DIA) to coordinate an investigation. According to Calder, the DIA nominee for Director of that organization contacted Slatkin and demanded an explanation of the CIA's actions. Subsequently, O'Neil requested that DDA Calder rescind the CIA letter. Calder states that O'Neill commented the actions of CIA security officials appeared to be "vindictive and malicious."
[19] C/SIB noted that he did not review Deutch's official security file. OIG reviewed the file.
[20] There is no record of Deutch receiving a code of conduct briefing. The Center for CIA Security provided an SCI briefing to the Commission members on two occasions. Deutch was present for the second one-hour presentation on November 17, 1998.
[21] Although HR 7-1 Annex D was superceded by the MOU on August 2, 1995, the current version of HR 7-1 Annex D is dated December 23, 1987 and does not reflect the changes caused by the subsequent MOU.
[22] According to paragraph II B.1 of the MOU, an "employee" is defined as "a staff employee, contract employee, asset, or other person or entity providing service to or acting on behalf of any agency within the Intelligence Community.
[23] According to paragraph II E. of the MOU, "'Reasonable basis' exists when there are facts and circumstances, either personally known or of which knowledge is acquired from a source believed to be reasonably trustworthy, that would cause a person of reasonable caution to believe that a crime has been, is being, or will be committed."
[24] Records of the Office of General Counsel indicate there were an average of 200 written crimes reports submitted to DoJ each year for the period 1995-1998.
[25] Title 18 U.S.C. §§793(f) and 1924 both prohibit the improper removal of "documents."
[26] A check of O'Neil's "sensitive personal file" was conducted by his secretary's successor in OGC. There was no evidence of any document regarding contact between O'Neil and the FBI General Counsel concerning a possible crimes report on Deutch.
[27] "811" is Section 811 of the Counterintelligence and Security Enhancement Act of 1994.
[28] The PDGC has served in the CIA since 1982. (She) was appointed PDGC, the second highest position in the Office of General Counsel, in the summer of 1995, and serve in that capacity until March 1, 1999. While serving as PDGC, (she) also served as Acting General Counsel from August 11, 1997 until November 10, 1997.
[29] The then-Executive Assistant to the GC states he was aware of the inquiry regarding the classified information found on Deutch's computer and that it was being worked by others in OGC. The Executive Assistant does not remember assisting the PDGC in this matter, but concludes that, if the PDGC states that he assisted her, he has no reason to doubt her recollection.
[30] The statue contains the pertinent phrase "and with the intent to retain such documents or materials at an unauthorized location."
[31] A crimes report was made by letter to DoJ on December 13, 1996. It is signed by the AGC in the Litigation Division, who was the OGC focal point for crimes reports at that time.
[32] Title 18 U.S.C.§793(f) and Title 18 U.S.C.§798 are felonies; Title 18 U.S.C. §1924 is a Class A misdemeanor.
[33] Title 28 U.S.C. §591(b)(7) limits applicability of the statue to the term of office of the "covered person" and the one-year period after the individual leaves the

office or position. This means that Deutch's potential exposure to the provisions of the Independent Counsel statue expired following the one-year anniversary of his resignation, which was December 14, 1997.

[34] The Intelligence Oversight Board is a standing committee of the President's Foreign Intelligence Advisory Board.

[35] The Group of Four refers to the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, and the two appropriations committees—the Senate Appropriations Committee, the Subcommittee on Defense and the House Appropriations Committee, National Security Subcommittee.

[36] Although O'Neil states he left the Agency in July 1997, he was present for duty until August 11, 1997 when he was replaced by the PDGC as Acting General Counsel.

[37] Hitz served as CIA IG from October 12, 1990 until April 30, 1998, when he retired.

[38] The former C/DCI Administration provided a copy of his MFR to Hitz, Calder, and C/SIB.

[39] A review of Hitz's files, which he left when he retired, failed to locate (the) MFR of the former C/DCI Administration or any notes or correspondence with this investigation.

[40] Hitz corroborates the OPS Legal Advisor's account of this meeting.

[41] C/SIB later explains, his use of the word "particulars" meant that he did not disclose what evidence had been discovered in his investigation. He states that it does not necessarily mean that Deutch's name and/or title was not discussed.

[42] On February 5, 1997, Hitz sent a memorandum to the Director of Personnel Security, Subject: "Crimes Reporting and Other Referrals by Office of Personal Security to the Office of Inspector General." The memorandum eliminated the requirement for OPS to routinely notify OIG of certain specific investigative matters in which it is engaged. Included as one of the nine categories of investigative issues identified in the memorandum was the following: "Mishandling of classified information that is or could be a possible violation of 18 U.S.C. 1924, 'Unauthorized removal and retention of classified documents or material.'"

DOE Counterintelligence Failures

In the wake of the reports by the Cox Committee (*see Chapter I*) on Chinese nuclear espionage and PFIAB (s*ee The Rudman Report on page 343*) on security lapses at DOE's nuclear weapons laboratories, and in response to Presidential Decision Directive NSC 61,[1] a comprehensive reform of counterintelligence (CI) at DOE was undertaken. This was accelerated and significantly refined in response to legislation proposed by Congress, which, among other things, created the National Nuclear Security Agency (NNSA).

The Permanent Select Committee on Intelligence of the House of Representatives established a bipartisan investigative Panel to examine DOE's plan to improve its CI posture at its headquarters in Washington and its three key weapons laboratories. The scope of the Panel's investigation was to determine what has been done by DOE and its key constituent nuclear weapons laboratories to improve CI policy and practices in the wake of the nuclear espionage investigation at Los Alamos National Laboratory, as well as to review the status of reforms and to examine issues still unresolved or under consideration. A special staff consultant, Paul Redmond, a former chief of CI at CIA, headed the team.

Upon conclusion of its investigation into DOE security and CI issues, the Redmond Panel presented its conclusions before the Committee and provided its evaluation on the state of CI at DOE and its key weapons laboratories at Los Alamos, Sandia, and Lawrence Livermore.

In general, the review determined that DOE had made a good but inconsistent start in improving its CI capabilities. The most progress had been made in building an operational CI capability to identify and neutralize insider penetrations. The two areas of greatest shortcoming, either of which could derail the whole CI program, were in CI awareness training and in gaining employee acceptance of the polygraph program. In spite of progress in some areas, the Redmond Panel also found unsettling the statements put forth by DOE Headquarters, claiming that counterintelligence problems had been solved. Failures and deficiencies caused by decades of misfeasance and neglect cannot be fixed overnight. The real test for assessing the CI program will be its future success in catching spies and security violators.

The Redmond Panel's report was entitled *Report of the Redmond Panel: Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories*, House Report No. 106-687, 21 June 2000.

R E P O R T of the REDMOND PANEL

IMPROVING COUNTERINTELLIGENCE CAPABILITIES AT THE DEPARTMENT OF ENERGY AND THE LOS ALAMOS, SANDIA, AND LAWRENCE LIVERMORE NATIONAL LABORATORIES

June 21, 2000—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
79-006 WASHINGTON: 2000

LETTER OF TRANSMITTAL

Permanent Select Committee on Intelligence,
Washington, DC, June 21, 2000.
Hon. J. Dennis Hastert,
Speaker of the House,
U.S. Capitol, Washington, DC.

Dear Mr. Speaker: Pursuant to the Rules of the House, I am pleased to transmit herewith a report submitted to the Permanent Select Committee on Intelligence of the House of Representatives by a team of investigators headed by the renowned expert in counterintelligence matters, Mr. Paul Redmond. The document is styled, "Report of the Redmond Panel: Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories." The Committee by majority vote earlier today authorized the filing of the report for purposes of printing.

Sincerely yours,
Porter J. Goss,
Chairman.

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE REPORT OF THE REDMOND PANEL "IMPROVING COUNTERINTELLIGENCE CAPABILITIES AT THE DEPARTMENT OF ENERGY AND THE LOS ALAMOS, SANDIA, AND LAWRENCE LIVERMORE NATIONAL LABORATORIES" FEBRUARY 2000

Executive Summary

In the wake of last year's reports by the Cox Committee[2] on Chinese nuclear espionage and by the President's Foreign Intelligence Advisory Board (PFIAB) on security lapses at the Department of Energy's (DOE's) nuclear weapons laboratories, and in response to Presidential Decision Directive NSC 61 (PDD-61),[3] Secretary of Energy Bill Richardson embarked on a comprehensive reform of counterintelligence (CI) at DOE. This was accelerated and significantly refined in response to legislation proposed by Congress which, among other things, created the National Nuclear Security Agency (NNSA).

The House Permanent Select Committee on Intelligence established a bipartisan investigative team in the first quarter of FY 2000 to examine the Department of Energy's plan to improve its counterintelligence posture at its headquarters in Washington and its three key weapons laboratories. The purpose of the examination was to review the status of reforms and to examine issues still unresolved or under consideration. The team was comprised of a majority staff member, a minority staff member, and a special staff consultant, Mr. Paul Redmond, one of America's leading experts in CI and a former head of CI at the Central Intelligence Agency (CIA).

In general, the review determined that DOE has made a good but inconsistent start in improving its CI capabilities. The most progress has been made in building an operational CI capability to identify and neutralize insider penetrations. The two areas of greatest shortcoming, either of which could derail the whole CI program, are in CI awareness training and in gaining employee acceptance of the polygraph program.

Among the specific findings and recommendations from the review are:

The current director of CI at DOE is an excellent choice for the job. Moreover, he has access to and the support of the Secretary.

DOE has failed to gain even a modicum of acceptance of the polygraph program in the laboratories. DOE must involve laboratory management in deciding who will be polygraphed.

DOE's efforts to improve CI awareness training have failed dismally. In developing its CI awareness training program, DOE should draw on the positive experience of other U.S. government agencies, in particular the CIA and National Security Agency (NSA).

DOE also faces a considerable challenge in the area of cyber CI, that is, protecting classified and sensitive computerized media databases and communications from hostile penetration. This will require significant investment in defenses and countermeasures and require the assistance of other federal agencies.

DOE CI has established an excellent, well-staffed, and effective annual CI inspection program that will serve to ensure the maintenance of CI standards and continued improvements in the program.

The "shock therapy" of suspending the foreign visitor and assignment programs worked in making the laboratories realize the degree to which these programs, if not properly managed, can be a counterintelligence threat. The CI components at the laboratories now appear to be better involved in the process of granting approvals for visits and assignees.

Cooperation at each laboratory between CI and security personnel is largely informal and

dependent upon personal relationships. DOE and the laboratories must establish more formal mechanisms to ensure effective communication, coordination, and, most importantly, the sharing of information.

The CI offices at the laboratories are hampered by their not being cleared for access to certain Special Access Programs (SAPs). Thus, the CI components are unable to exercise CI oversight of these activities. The Director of Central Intelligence (DCI) should work with the DOE Secretary to remedy this situation.

DOE needs to establish contractual CI performance standards for the laboratories against which they can be judged and duly rewarded or penalized.

It should be noted that the Committee has not adopted the Redmond Panel's position in favor of the maintenance of the current centralization of all CI authority at DOE for a short, transitional period.

Introduction and scope of investigation

The scope of the team's investigation was to determine what has been done by the Department of Energy (DOE) and its key constituent nuclear weapons laboratories to improve counterintelligence (CI) policy and practices in the wake of the nuclear espionage investigation at Los Alamos National Laboratory. The team was limited to evaluating CI capabilities at the three principal nuclear weapons laboratories at Los Alamos, Sandia, and Lawrence Livermore, and at DOE Headquarters. The team was also to propose additional measures to improve CI at those facilities if, in the judgment of the team members, such measures were warranted.

The team interviewed DOE officials in Washington, D.C., California, and New Mexico. It also interviewed contractor employees of DOE, including employees of the University of California and Lockheed-Martin, at the three nuclear weapons laboratories. In addition, the team interviewed numerous officials of the Federal Bureau of Investigation (FBI), both at FBI Headquarters and at FBI Field Offices in San Francisco, California and Albuquerque, New Mexico, and officials of the Central Intelligence Agency (CIA) and the National Security Agency (NSA).

This report is not linked to DOE's own progress reports, which cite percentages of CI steps that DOE considers to be "implemented" at the three weapons laboratories. The team quickly determined that DOE used imprecise terms in describing the results of its self-evaluation. For example, the word "implemented" is commonly understood to mean that something has actually been accomplished, whereas DOE considers a CI directive as implemented when it has only been promulgated. For instance, in a September 1999 progress report, DOE claimed to have implemented the recommendation that lab CI offices contact all employees and contractors who have met with foreign nationals from sensitive countries. From its on-site visits the team determined that, although the laboratory CI offices are aware of the recommendation, they have yet to carry it out. The team thus does not believe that DOE's evaluative methodology is useful in assessing the true extent to which CI measures have been "implemented."

Historical comment: In the course of interviewing numerous laboratory personnel, the team encountered a pervasive, but muted, sentiment that many of the CI and security problems at the laboratories were exacerbated, if not caused, by the policies of former Energy Secretary Hazel O'Leary. These policies included the redesign of laboratory identification badges that resulted in the intentional obscuring of distinctions between clearance levels, the collocation of Q-cleared personnel with individuals who held lesser clearances, and the widespread use of "L" clearances--which still require only the most cursory background check for approval. One senior lab official opined that the L clearance program was "the worst idea in government--cursorily clearing people who didn't need access to Q material created new vulnerabilities."

The team notes that DOE was not unique in de-emphasizing basic security procedures in the wake

of the end of the Cold War. The State Department, for example, embarked on its now infamous "no escort" policy, the Defense Intelligence Agency issued "no escort" badges to Russian military intelligence officers, and even the Central Intelligence Agency precipitously abandoned its policy of aggressively recruiting Russian intelligence officers. The present and future Administrations must ensure that such laxity will never again be encouraged or tolerated.

DOE Office of Counterintelligence (DOE CI)

Presidential Decision Directive NSC 61 (PDD 61), issued on February 11, 1998, provided for the establishment of a new DOE CI program that reports directly to the Secretary of Energy. In April 1998, DOE's CI office became operational. Under the guidance of the director of DOE CI, Mr. Edward Curran, the Department has made considerable progress towards establishing an effective CI operational capability at DOE Headquarters to do the analytical and investigative work necessary to identify and neutralize insider penetrations. It is the team's opinion that Mr. Curran is ideal for the CI director job because of his extensive CI experience at the FBI, his rotational assignment at the CIA, and his persistence and determination. [EDITOR'S NOTE: At the end of 2000, Ed Curran retired after rebuilding DOE's counterintelligence program. In June 2001, Michael Waguespack was appointed to succeed Curran. Waguespack was serving as a deputy assistant director of the FBI's National Security Division before his appointment.]

Mr. Curran appears to have access to and the support of the Secretary of Energy, which is an essential ingredient to an effective CI program. Moreover, he is vigorously attempting to exert DOE CI authority and influence over the laboratories, which, while difficult to accomplish, is critical to the success of the new CI program. In the future direct access to the Secretary and close working relations with other offices reporting directly to the Secretary, including the Offices of Security Affairs and Intelligence will be crucial. In addition, DOE CI must establish and maintain a mutually supportive relationship with the Office of Independent Oversight and Performance Assurance, which performs inspections of DOE programs and policies. This office has an established record[4] of detecting, documenting and reporting CI and security shortcomings at the laboratories. Regrettably, past findings of this office in the CI realm evidently were rarely acted upon. This office, which is philosophically attuned to CI and security issues, now has a good working relationship with DOE CI and has recently pointed out at least one CI cyber security[5] vulnerability. In the future, the office will be a natural ally for DOE CI as it tries to assert authority, identify problems and implement new policies.

Mr. Curran is hiring and, where necessary, training a good cadre of CI officers to perform investigations from DOE Headquarters. The CI components at the laboratories,[6] moreover, seem well on the way towards adequate staffing. Laboratory interaction with the FBI appears to be effective, at both the management and CI component level. That said, laboratory CI offices will need to focus for the foreseeable future on (1) gaining the confidence of their laboratory colleagues; (2) crafting CI programs that fit the unique needs of each lab; and (3) conforming to DOE's requirements for more standardized approaches and procedures. The team appreciates that the job of reforming CI at DOE and the laboratories will require steadfast resolve on the part of Mr. Curran and his successors, continued support from the Secretary, and sustained resources from Congress.

Congressionally mandated reorganization of DOE

Mr. Curran believes that any authority he may have had in his new job as DOE's director of CI will be greatly diluted by the new structure established in the National Defense Authorization Act for Fiscal Year 2000. While the team will not attempt to evaluate the restructuring plan, Mr. Curran's views on the matter remain germane to the team's evaluation of how DOE Headquarters is approaching CI reform at the laboratories.

Mr. Curran indicated to the team that his initial plan had been to place federal employees rather than contractors as the CI chief at each laboratory. This would, in his view, create a more disciplined line of authority necessary to counter the historical unresponsiveness of the laboratories to DOE Headquarters directives. Mr. Curran ultimately accepted the argument put forth by the laboratories, however, that laboratory employees, i.e., contractors, would be more acceptable locally and would thus be more effective.

Mr. Curran believes that given the semi-autonomous status of new National Nuclear Security Agency (NNSA) under the statutory restructuring, he will have only a policy role and no actual authority over these contractors. In his January 1, 2000 implementation plan, the Secretary proposed that the present director of DOE CI serve concurrently both in that capacity and as Chief of Defense Nuclear CI in the NNSA.

Separation of CI and security disciplines at the laboratory level

The deliberate separation of CI and security disciplines at the laboratories as advocated by DOE Headquarters senior management and as legislated by Congress could cause problems both at Headquarters and the laboratories. Management at each of the laboratories has sensibly placed CI and security where the expertise is. For instance, cyber security at all three laboratories resides under information management for organizational purposes. At Lawrence Livermore, the CI component resides under operations. Laboratory management and the CI chiefs appear satisfied with such arrangements. They uniformly indicated that security and CI are connected by what one Lawrence Livermore manager described as "multiple neurons" under such a rubric as an "Operational Security Group." This group ensures that each interested or responsible component is informed and involved as issues arise.

Such claims notwithstanding, the team discovered that these "multiple-neuron-type" arrangements are not formalized in any meaningful way at any of the three laboratories. In each case, the communications arrangements appear to depend primarily on personal and working level relationships. It has been the sad experience in many espionage cases that only after the spy is uncovered, does it become clear that a plethora of counterintelligence indicators concerning various facets of the individual's life, performance, and behavior, had been known in different places by different individuals, but never effectively collated or holistically evaluated.

DOE must ensure that the CI officers at the laboratories are part of a formal system set up locally to ensure that all relevant CI and security data information is collected, assembled, and analyzed by means that are not solely dependent on personal relationships. Otherwise, the retirement or transfer of one individual in the process could cause the whole system to break down. Without an effective organizational structure, there is no guarantee that all relevant data will become known to the CI office.

The team is not satisfied that DOE and the laboratories have completely grasped this concept. Moreover, the DOE Operational Field offices at Albuquerque and Oakland continue to refuse to share relevant information from employee personnel files under their control with DOE CI or laboratory CI components. The team learned that DOE CI is not even informed by these three offices when an employee loses his or her security clearance. Therefore, the team recommends that DOE ensure that a formal communications process for CI information between and within the laboratories and between DOE Operational Field offices and CI personnel be established immediately.

CI inspection teams

PDD-61 requires an annual inspection of DOE's CI program. DOE CI has hired and deployed a dozen retired FBI, CIA, and military intelligence officers to inspect the CI programs at the three weapons laboratories. This excellent initiative is already yielding promising results by identifying systemic

problems and offering solutions. The inspection team consists of highly experienced individuals, who appear to be insulated from the politicization that can yield watered down findings. The team's effectiveness, however, will be largely dependent upon the frequency of its inspections. We recommend that DOE continue annual inspections as stipulated in PDD-61 and add follow-up inspections focusing on specific problem areas. The team judges that there is no DOE CI program that is more useful or efficient than this inspection regime. We recommend, therefore, that resources adequate to expand this inspection program be provided.

The inspectors have reasonably noted that since they are just beginning their program, they should focus on establishing a baseline for assessing where the laboratory CI programs should be within a year or so. The reaction at the laboratories to these inspections has been generally favorable, with only minor complaints about repetitious questioning and an over-reliance on the format of a standard FBI internal inspection that is not entirely appropriate for this effort. Some of the CI chiefs at the laboratories believe that the inspection teams, employing a narrow FBI focus, put too much emphasis on laboratory investigative capabilities and not enough on the information gathering, non-law enforcement role of the laboratory CI units. Also, the capability of the inspection teams in the difficult, arcane cyber area needs enhancement. Overall, however, this is a fine program. With some minor adjustments, it should become an effective instrument to ensure the continued improvement of CI at the laboratories.

Polygraph testing

Polygraph testing for "covered"[7] DOE and laboratory personnel was mandated by Congress, but DOE Headquarters reacted with poorly thought out and inconsistent directions to implement the requirement. As a result, laboratory personnel have a very negative attitude towards the polygraph. Moreover, since the polygraph is a highly visible part of the overall CI effort, the entire CI program has been negatively affected by this development. At the center of this problem is DOE's lack of success in explaining the importance and utility of the polygraph program. Further exacerbating this problem, DOE Headquarters personnel made little effort to consider the views of senior laboratory managers and have not involved them in the planning process for determining who will be polygraphed. In addition, DOE Headquarters efforts to meet with the laboratory employees to explain the polygraph program have been ineffective, if not counterproductive. To make matters even worse, DOE Headquarters, by vacillating and changing the policy over time, appeared inconsistent and unsure where the opposite is essential to instill confidence in the program parameters and professionalism.

The attitude toward polygraphs at the laboratories runs the gamut from cautiously and rationally negative to emotionally and irrationally negative. Moreover, the attitudes of the lab directors themselves range from acknowledgement of the need (although uncertain as to how to implement it), to frank and open opposition. Scientists at Sandia prepared a scientific paper purporting to debunk the polygraph for a laboratory director's use in a Congressional hearing. Employees at Lawrence Livermore wear buttons reading "JUST SAY NO TO THE POLYGRAPH." Other laboratory employees expressed the sentiment "You trusted me to win the Cold War, now you don't?" The team heard such statements as, "The Country needs us more than we need them" and "The stock options of Silicon Valley beckon." Several expressed a belief that many scientists will quit and that DOE will not be able to maintain the stockpile stewardship program. Still more employees cited an Executive Order that exempted Presidential appointee and "Schedule C" employees from having to take the polygraph as outrageous and unfair.

In addition to the emotional reactions, there are rational questions about the polygraph, such as, "What are they going to do with the inevitable number of people who do not pass?" The team shares this concern, and expects that there will be a significant number of so-called "false-positive" polygraph results that will have to be further

examined. Another concern voiced to the team by numerous laboratory employees was that "No one has ever tried this before on this scale." The fact is that never before have so many "cleared" employees of a government organization had to have their clearances (and, thus, their livelihoods) threatened by the institution of the polygraph.

Compounding the problem further is an attitude among many laboratory employees that they are indispensable and special, and thus, should be exempt from such demeaning and intrusive measures as the polygraph. Scientists do, in fact, represent a particular problem with regard to the administration of polygraphs. They are most comfortable when dealing with techniques that are scientifically precise and reliable. The polygraph, useful as it is as one of several tools in a CI regime, does not meet this standard. Accordingly, many scientists who have had no experience with it are skeptical of its utility.

DOE's efforts at explaining the utility of the polygraph as part of a multi-faceted CI program have been ineffectual. Moreover, DOE Headquarters' response to resistance at the laboratories, as unreasonable as that resistance may be, has been dictatorial and preemptory. As one senior DOE official observed, on hearing the complaint by the laboratories that the polygraph will make it difficult to recruit and retain top scientists, "It is already difficult to recruit and retain scientists in this economy, so what's the difference?"

In December 1999, the Secretary announced that DOE intends to reduce the number of employees subject to the polygraph to about eight hundred. This change, coupled with the elimination of the exclusion for senior political appointees, indicates that DOE Headquarters is trying to rectify the original overly broad and impractical scale of the polygraph program. Nonetheless, even this well-intentioned step has elicited skepticism. As one senior manager said, "What is to prevent some new Secretary from coming along and hitting us for not polygraphing all thirteen thousand laboratory employees?"

The team judges that DOE Headquarters should do more to involve laboratory management in the process of selecting those individuals to be polygraphed. Senior laboratory managers know what secrets need protecting and, thus, could bring their knowledge to bear on this process. Including managers visibly will involve them with the program in the eyes of the workforce. This will both motivate and enable them to sell the program, and, one hopes, give the program more credibility. Their participation, moreover, would make them accountable.

To this end, DOE must reinvigorate and revamp its effort to educate the workforce on how polygraphs, while not definitive in their results, are of significant utility in a broader comprehensive CI program. The polygraph is an essential element of the CI program and it will not work until it is accepted by those who are subject to it.

Counterintelligence awareness training

There has been no discernable, effective effort from DOE Headquarters to establish and support an effective CI training and awareness program. Moreover, the team was unable to identify any real efforts on the part of DOE CI to improve upon existing DOE training and awareness practices for laboratory employees.

No organization, governmental or private, can have effective CI without active, visible, and sustained support from management and active "buy-in" by the employees. It is not possible to do CI by diktat, or from a distance. In the words of one DOE officer, the CI program cannot be a success unless each employee "knows the requirements [of the program], his or her own responsibilities, and is trained to carry them out."

Historically, the laboratories have--on their own initiative--sponsored CI and security lectures and briefings to supplement the annual security refresher required of each employee. The CI lecture series at Lawrence Livermore is an excellent program. Unfortunately, it has not been replicated by the CI offices at Sandia or Los Alamos, which instead

sporadically arrange ad hoc presentations. Moreover, the annual security refresher, which these lectures supplement, is perfunctory and pro forma. It can consist of as little as a brief presentation on a personal computer followed by a short quiz to ensure that the employee has read the material. As a result, the refresher process is not taken seriously by the employees, especially since DOE Headquarters has dictated much of the content in the past without consulting the laboratories. The sample training materials examined by the team were bureaucratic, boring, turgid, and completely insufficient.

The poor state of the training program is also reflected in the mistaken belief by CI officials in Washington that a training facility at Kirtland Air Force Base in Albuquerque, New Mexico, is assisting in developing CI teaching materials for DOE's next annual refresher. When contacted by the team, the facility indicated that it was playing no such role. Clearly, DOE CI has yet to turn its attention to improving CI training.

In lieu of a department-wide program, the laboratories have taken some uncoordinated initiatives to meet some of their awareness training requirements, if only in response to the uproar caused by events at Los Alamos. Management at all three laboratories appears to have given some thought, at least, to what may be required. Managers have drawn an analogy between their successful occupational safety training and awareness program and how they are to make security and CI an accountable, integral part of each employee's daily work and professional mindset. At Sandia and Los Alamos, specifically, management recognizes that, as in safety management, it should give line managers specific roles and responsibilities for CI and security, and then hold them accountable. This would appear to be a constructive step.

The View from the Laboratories

Laboratory management made the following comments regarding training and awareness:

"Some of the awareness training material received from Washington is so bad it is embarrassing. Were it used, it would undermine the credibility of the whole program."

"We had to scramble to find speakers on the subject [of CI during a lab-wide CI and security stand-down]."

"One [CI] lecture given by an experienced former FBI agent, tailored to the laboratory audience, was a huge success. We need more of this sort of thing."

"There is no line budget item for training, each speaker costs about $4,000, yet there is no Headquarters-generated program."

"DOE Headquarters' approach to training and awareness has been form over substance, represented by dictated programs and policies."

"There is an acute need for 'realistic' awareness training, so people will realize the problem did not go away with the Cold War and they are still targets."

"There are [laboratory] divisions standing in line for tailored presentations."

"Concrete examples, real [CI] incidents, and their consequences are required to get people's attention. They [the scientists] must be captured intellectually."

In the spring of 1999, the Secretary issued a series of short-notice security, CI, and cyber-related "stand-downs" at the laboratories. This was not well received by laboratory employees. Some characterized the stand-downs as a "frog marching exercise" that discredited the whole effort at improving CI by alienating significant parts of the workforce. An exception to this belief was at Los Alamos, where the stand-downs were viewed as a "unifying" experience--presumably because of the siege mentality that existed there in the wake of the nuclear espionage allegations.

The CI component at DOE Headquarters has a new training officer, and the office apparently intends to develop a program to support CI awareness and training at the laboratories. One starting point would be to follow the example of other successful CI training programs. CIA, in the aftermath of the Aldrich Ames espionage case, also instituted a very aggressive CI course and lecture program supplemented by an in-house television series. In addition, NSA has a long-standing, effective training and awareness program that the team examined at length prior to its field visits to the laboratories.

It is instructive to consider the experiences of NSA, particularly in dealing with the parts of NSA populated with an accomplished collection of world-class mathematicians and cryptologists. This highly skilled workforce is very similar to that found at the laboratories. The key factor in NSA's success in the training and awareness area appears to be that its overall integrated security and CI program has been in existence for many years, and the mathematicians enter a culture where, from the very beginning of their employment, security, CI, and the polygraph are "givens" in their daily work. DOE is now starting virtually from scratch and would do well to learn from the positive experiences of agencies such as NSA.

NSA has also had success with a program designating a security and CI referent for each significant component. This individual is not a security professional, but a regular employee of the component, one of whose additional duties involves dealing with security/CI issues. The referent, who receives some extra security and CI training, is partly rated on his performance in this role and is responsible for selling the CI program at the lowest bureaucratic level. This system, by all accounts, has been quite successful. Los Alamos has a large number of employees who are responsible for "security" in their units. Their role at Los Alamos could be expanded along the lines of the NSA model and could be adapted elsewhere. The team also notes that when it raised NSA's security/CI referent concept at each laboratory, there was widespread interest in it. Resources to enable the laboratories to institute a referent program along the lines of the NSA model should be provided.

DOE Headquarters must do much more to support field training and awareness by establishing a comprehensive curriculum for use by the laboratories that is interesting and substantive enough to catch the attention of the difficult laboratory audience, and sufficiently flexible to allow individual CI directors to address the specific needs of each laboratory. In addition, DOE should establish a CI training course for managers. Like the successful occupational safety management training, this course should emphasize that CI is an integral part of each manager's job.

Finally, Congress should support extensive CI training and awareness programs at DOE Headquarters and the laboratories. This should include providing funds specifically for this purpose in FY 2001 to ensure that training and awareness needs are met and that money is not diverted to other programs. Congress should carefully oversee the implementation of the program it funds to ensure that training and awareness becomes, and remains, a high priority for DOE.

Cyber CI

DOE and the weapons laboratories face their biggest challenge in the area of cyber CI. The magnitude of the problem and the complexities of the issues are daunting. There are several thousand systems administrators at the laboratories who have very wide access. There are each day hundreds of thousands of internal e-mails at the laboratories and tens of thousands sent to external addresses. Additionally, there are extremely complicated issues of connectivity and systems architecture. The laboratories, wherein reside massive brainpower and experience in cyber matters, are beginning to address this challenge cooperatively and, in some cases, with the assistance of other U.S. Government agencies. Some laboratories have in place programs using "key words" to scan e-mail traffic for CI indicators, but it is too early

to formulate any substantive judgments of their effectiveness.

It is clear that DOE CI has not yet fully established its authority at DOE Headquarters and at the laboratories in the cyber area. The cyber component of DOE CI is trying to overcome legal obstacles centering largely on privacy issues related to implementation of a pilot program to determine the size and difficulty of e-mail monitoring using sophisticated "visualization" software. There is another pilot program under development to detect cyber intrusions better. DOE CI is encountering bureaucratic resistance to establishing acceptable minimum standards. For instance, the laboratories are pressing for standards that are acceptable in a more open "academic" environment. Furthermore, a comprehensive intrusion incident reporting mechanism for the computer systems controlled by DOE information management offices and the laboratories is meeting resistance from DOE and laboratory personnel, who cite excessive reporting burdens.

There has existed for years at the laboratories an entity called the Computer Incident Advisory Capability (CIAC) that was responsible for collecting and analyzing computer security incident data. The reporting to this organization has historically been voluntary, and anonymity was permitted to encourage the laboratories to be frank and forthcoming. More recently, the CIAC has begun to provide DOE Headquarters with intrusion incident summaries. The lack of specificity in these summaries, however, makes meaningful analysis impossible. DOE CI, with assistance and support from DOE management, needs to assert its authority in this matter.

It appears that DOE CI is very well served by employing detailees from the FBI and NSA. These detailees bring a high-level of expertise to the issue and some independence from DOE's bureaucracy. The practice of assigning them to play a leading role in the cyber CI component should be continued.

The DOE CI component believes that it has an effective working relationship with DOE's Office of Independent Oversight and Performance Assurance. This office conducts "red team attacks" on the computer systems and has helped impose computer security standards at the laboratories. Clearly, the functions of DOE CI and this office are complementary, particularly in the cyber area. This close working relationship will be a key to improving overall cyber CI.

In sum, DOE CI, faces in the cyber area, the same very difficult, complicated issues faced everywhere in the national security community. The individuals who create and run computer systems are, by training and motivation, inclined to promote the widest, fastest, most efficient dissemination and transmission of data; hence, the basic and pervasive mutual aversion between "Chief Information Officers" and the security/CI offices. The team believes that adequate resources should be provided for cyber security and CI, and that aggressive oversight should be exercised to ensure that effective programs are developed and implemented.

Foreign visits and assignments

The team limited its examination of this issue to the role played by DOE CI and the laboratory CI offices in the visitor and assignments approval process, which would lead to the laboratory director seeking a "waiver" to the moratorium on foreign visits from sensitive countries. The team notes that Secretary Richardson announced in December 1999 that he might start seeking such waivers as permitted by the FY 2000 National Defense Authorization Act.[8] All three laboratory CI chiefs stated that they now have an established, integrated role in the approval process leading to a laboratory director seeking a waiver to allow such a visit. For instance, the CI chief at Lawrence Livermore is one of four officers who must sign off before a request goes to the laboratory director for a decision to seek a waiver. The CI chief at Sandia is a member of the Foreign Visits and Assignments Team, which actually controls the approval process. These officials can thus bring to bear a CI perspective on any proposed visit, which the team believes to be a crucial function.

Obviously, the judgments made by the laboratory CI offices are only as good as data on which they are based. These data includes indices checks, which have often been slow in coming from other Federal agencies. The laboratory CI offices need to have access to broader-based intelligence information. This information, when integrated by the analysts in the CI offices, would give them a much improved basis on which to judge the CI threat that individual visitors and delegations might pose. Access to this information is problematic, and DOE CI needs to work with other relevant entities at DOE Headquarters—particularly the Office of Intelligence—to arrange appropriate and efficient access in the field.

In addition, there are two relevant databases. The Foreign Assignments Records Management System (FARMS) is unclassified and is maintained by DOE security. The Counterintelligence Analytical Research Data System (CARDS) is maintained by DOE CI and is an outstanding repository of classified data on prospective foreign visitors. Laboratory CI offices believe that they need a "bridge" between these databases so they can more effectively use the information they contain. In addition, it appears that the laboratories, which in some cases maintained their own databases, feel less confidence in the quality of DOE-maintained data, and their access has become more cumbersome. DOE CI needs to address these problems.

Apparently, the legislatively imposed moratorium on foreign visits and assignment has had the desired effect of making DOE and the laboratories much more conscious of the CI threat posed by visits.[9] Making the laboratory directors accountable has also had a salutary effect. It now remains for DOE CI and the laboratory CI offices to work together to make sure the CI role in the approval process is made as effective as possible by bringing to bear the maximum amount of data as efficiently as possible. There will also need to be more awareness training to sustain and better improve the presently enhanced levels of interest and attention.

CI knowledge of special access programs (SAPs) and other sensitive projects

The laboratories do a considerable amount of work for the Intelligence Community under the auspices of the "Work-for-Others" program. This work, administered by DOE, is often highly sensitive and is administratively compartmented within SAPs, which require additional clearances. The laboratory employees who work on these SAPs or other projects technically fall under the CI jurisdiction of the laboratory CI office. The team discovered inconsistencies in this arrangement in two of the laboratories that could lead to potentially dangerous outcomes for CI if not corrected.

At Lawrence Livermore, laboratory CI officials are not permitted to become involved in the "Work-for-Others" programs involving Intelligence Community SAPs. They are not substantively or administratively informed of any aspect of the programs. Given that one of the primary functions of the laboratory CI staff is to brief employees on CI threats and to inquire about CI incidents, the CI office at Lawrence Livermore is unable to perform fully this critically important function. Lawrence Livermore's CI chief advised that he learns of "Work for Others" activities only "by mistake" or "by accident." In some instances when he has tried to involve himself in issues related to "Work-for-Others" activities, he has been restrained by his senior management, which presumably is seeking to enforce Intelligence Community requirements. A similar situation prevails at Sandia, where it was evident that the CI component is often unaware of "Work-for-Others" activities.[10]

The net result of this situation at Lawrence Livermore and Sandia is that no one appears to be examining CI issues involving personnel engaged in the most sensitive SAPs and other Intelligence Community projects without a formalized reporting mechanism, there is no guarantee that an employee will report a CI incident to the contracting intelligence agency. The contracting agency, may or may not, in turn, report the problem or issue

to the DOE Office of Intelligence, DOE CI, or to FBI Headquarters. The team judges this to be an unacceptable process for the transmission of such critical CI information. DOE Headquarters should reach a formal agreement with the Intelligence Community to ensure that the laboratory CI offices are read into the SAPs at least at an administrative level so they can fulfill their CI responsibilities. The team also encourages the Community Management Staff (CMS), which has been tasked by the Director of Central Intelligence (DCI) to examine the protection of Intelligence Community equities by DOE and the laboratories, to work closely with DOE to resolve this issue of the lack of a formalized reporting mechanism.

Sensitive unclassified technical information (SUTI)

DOE has instituted a new pseudo-classification for material that is deemed sensitive, but is technically unclassified. The team encountered significant confusion at the laboratories about what will actually be captured under the SUTI category, and laboratory managers expressed strong opposition to the whole concept. One principal argument was that scientists who work at the laboratories are already precluded from publishing much of their work because it is classified. The scientists often feel that much of what they must treat as classified is actually publicly available and being discussed by their non-U.S. Government peers around the world. Also, given that their scientific reputations are largely dependent upon what they publish and upon their interactions with their non-U.S. Government peers, they feel that the SUTI category further prejudices their ability to earn scientific recognition. Moreover, laboratory employees pointed out to the team that the SUTI category is highly subjective, cannot be standardized in any fair way, and will necessarily compel them to look for work outside of government if it is strictly imposed.

It appears that the DOE Headquarters policy on SUTI is evolving much like its policy on the polygraph, with similar misinformation, misunderstanding, and general confusion among those who will be affected by it. At Los Alamos, senior managers advised the team that SUTI was no longer an issue because it had been replaced with a DOE list of sensitive subjects. It is interesting that Lawrence Livermore and Sandia were, at the same time, still laboring under the assumption that they would be subject to SUTI and were making decisions based upon this assumption.

In the team's judgment, DOE should proceed very cautiously and openly on SUTI imposition--if it does so at all--so as to avoid repeating the internal public relations mistakes it made with the polygraph program. Moreover, it appears DOE has yet to address the significant legal implications associated with the promulgation and implementation of SUTI. This fact was acknowledged recently by DOE's General Counsel, who issued a notice stating that since "sensitive information" is neither defined in the National Defense Authorization Act for FY 2000, nor in DOE's existing regulations, DOE will not impose new statutory penalties associated with mishandling sensitive unclassified information. Therefore, until a clear and well thought out rationale and implementation plan has been formulated by DOE for SUTI--which must include engagement with laboratory management and personnel to be effective--the team believes that steps to implement SUTI regulations should not proceed.

Enforcement

Each contract DOE has with the operators of the laboratories requires an annual appraisal of performance. In the past, these appraisals apparently included an ineffective pro forma consideration of security. It appears that neither DOE Headquarters nor DOE Field Offices, which are directly responsible for contract oversight, effectively enforced the terms of the contracts in this area. For example, the team was told that in some instances the University of California was not consciously aware of the fact that it was contractually responsible for certain security provisions, even though these were explicitly stated in the contract. The team recommends that DOE enforce existing security performance measures. Further, the team recommends that

DOE incorporate measurable CI objectives and performance standards into each of its laboratory contracts. DOE could then use the previously mentioned CI audits, possibly combined with the findings of the Office of Independent Oversight and Performance Assurance, to evaluate the performance of the laboratories and impose penalties on the contractors for unacceptable performance.

The team understands that DOE is working on language for contracts that will allow DOE to assess CI performance at the laboratories. The initiative represents an incentive for the laboratories to perform, and an opportunity to put in place measures to remedy past poor performance by the laboratories in this area. The team believes that Congress should support, encourage, and oversee the initiative, and ensure that DOE rigorously enforces the CI standards that it sets out in its contracts.

Conclusions

Hostile intelligence threats to DOE and the laboratories will most likely come from problems with trusted employees, cyber penetrations, and visitors or assignees. DOE has made good progress toward establishing effective operational mechanisms to cope with the problems of identifying possible "insider" penetrations and of laying the groundwork for the FBI to investigate. DOE has also set up an excellent inspection system to ensure the continued efficacy of these mechanisms, but it is not yet clear that this system is being evenly applied across all CI and security programs.

DOE has not effectively laid the groundwork for acceptance of the polygraph program, an obviously essential part of any CI effort to detect and deter espionage by employees. Moreover, DOE has failed to establish the absolutely key, complementary CI pillar--an effective training and awareness program.

No CI program can succeed unless both the operational and training pillars are in place and supporting each other. Further, it is clear from decades of behavior, that the DOE and laboratory culture is profoundly antithetical toward CI and security. Unless changed, this entrenched attitude will doom any attempts at long-term improvements. Effective training and awareness programs are the only way to change this cultur
DOE is just beginning to determine the magnitude of CI issues relating to the cyber threat, which includes e-mail and intrusions. The cyber component of DOE CI needs strong support at DOE Headquarters to establish suitable, minimum CI standards in systems controlled by DOE's information management units and the laboratories.

Processes are now in place that should ensure that CI concerns will be factored into the waiver approval system for foreign visitors and assignments, questions of security in the approval process, however, were beyond the scope of this study.

In spite of progress in some areas, statements from DOE Headquarters, to the effect that all is now well in the CI area is nonsense. Problems and deficiencies caused by decades of nonfeasance and neglect cannot be fixed overnight. Such statements serve only to strengthen the position of those at the laboratories who would wait out the effort to improve CI and thus make the job all that much harder. Our yardstick for assessing the CI program will be their future success in catching spies.

Endnotes

[1] PDD-61 was issued on 11 February 1998 in response to GAO and Intelligence Community reports that found serious CI and security problems at DOE and its constituent laboratories.

[2] The Cox Committee's formal name was the House Select Committee on US National Security and Military/ Commercial Concerns With the People's Republic of China.

[3] PDD-61 was issued on 11 February 1998 in response to GAO and Intelligence Community reports that derided CI and security issues at DOE and its constituent laboratories.

[4] In 1994, this office discovered a serious vulnerability at Los Alamos—there was no technical or policy impediment to the transfer of classified data from a classified to an unclassified computer system. This finding was apparently duly documented and reported to the requisite DOE offices and to Congress. Disturbingly, no remedial action was taken.

[5] Cyber security is meant to encompass security for all computer systems at DOE and the laboratories.

[6] The term "laboratories" will hereinafter include only Los Alamos, Sandia, and Lawrence Livermore National Laboratories.

[7] Section 3154 of the FY 2000 Defense Authorization Act defines "covered" persons as those involved in Special Access Programs, Personnel Security and Assurance Programs, and Personnel Assurance Programs and those with access to Sensitive Compartmented Information.

[8] *Washington Post*, 3 December 1999, "Energy Chief To Allow Foreign Scientist To Visit Labs."

[9] Evaluating the security aspects of the visits and assignments program is beyond the team's remit and is therefore not addressed herein.

[10] Due to the communications arrangements between Los Alamos chiefs of intelligence, CI, and security, Los Alamos does not appear to have the same problem as Sandia and Lawrence Livermore National Laboratories.

Leaks

On 14 June 2000, the House Intelligence Committee held a hearing to review recent significant instances of the public release of classified information. The purpose of the hearing was 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 US satellite collection systems; and SIGINT information on terrorists, proliferation, and other targets.

The public release of such material usually results in the loss of access to intelligence; the enhancement of denial and deception techniques by foreign adversaries; 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 US Government's ability to obtain further information."

In most leak 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.

Although there are statutes prohibiting the unauthorized disclosure of certain types of information—diplomatic codes, nuclear information, communications intelligence, or "national defense" information—there is no general criminal penalty for the unauthorized disclosure of classified 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 apply to only classic espionage situations and are not meant to be applied to "leaks."

The House Intelligence 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 have prohibited 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.*

Proponents of the provision maintained that leaks of highly sensitive intelligence information had not only risk the loss of valuable collection capabilities but also jeopardized important security interests. Critics, on the other hand, argued that the provisions were overly broad and would preclude the type of leaks that in the past had ultimately benefited the American public.

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 13 November 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 6 December 2000, and the House passed the bill on 11 December 2000 without amendment. The President signed the bill on 27 December 2000 as P.L. 106-567.

Despite having lost on the "leak issue," the House Intelligence Committee said it would continue its oversight of efforts to prevent and investigate unauthorized disclosures of classified information and to reintroduce legislation in the 107th Congress to address the insufficient statutory prohibitions against leaks of classified information.

Senator Richard Shelby took the lead and drafted "antileak" legislation. Senator Shelby stressed that, unlike Britain's Official Secrets Act, his legislation targets only the "leakers." It "criminalizes the actions of persons who are charged with protecting classified information, not those who receive or publish it."

Opposition to Senator Shelby's legislation pointed out that, contrary to the senator's assurance, criminalizing disclosure of classified information has legal ramifications that went far beyond the leaker. The relevant statutes include 18 USC 2, which dictates that "Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal." This means that both the leaker and the one who elicited the leak could end up in jail.

Even the passive recipient of a leak could be in trouble if he does not immediately alert the authorities, according to 18 USC 4 ("Misprision of felony"). "Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined under this

title or imprisoned not more than three years, or both."

The effort to enact a criminal statute prohibiting the unauthorized disclosure of classified information ended when a hearing on the matter was canceled and the measure was withdrawn from consideration in the FY 2002 Intelligence Authorization Act.

Senator Shelby's office issued a terse statement:

> *At the request of Attorney General John Ashcroft, the Intelligence Committee has postponed Wednesday's hearing to study the leaking of classified information. The Justice Department has requested additional time to study this issue.*

Senator Shelby later commented that "This bill is going to be back in the hopper, if not by me then by others. This is not a this-year legislation, necessarily. It's long-term legislation. This legislation is not going away, because the problem [of leaks] is going to get worse, not better."

Timothy Steven Smith

On 8 April 2000, Federal authorities filed espionage charges against Timothy Steven Smith, a 37-year-old civilian Department of Defense employee assigned as an ordinary seaman aboard the USNS Kilauea, an ammunition ship that was moored at the time at the Puget Sound Naval Shipyard in Bremerton, Washington. Smith was accused of attempting to steal classified computer disks and documents from an officer's cabin on the ship on 1 April, apparently in an attempt to take revenge on shipmates who had mistreated him.

One of the five classified military documents stolen by Smith detailed the transfer of ammunition and the handling of torpedoes on board US Navy ships. Smith said that he wanted to steal "valuable classified materials" and then possibly sell them over the Internet to terrorist groups.

According to the *Seattle Post Intelligencer*, Smith pleaded guilty to reduced charges. As part of his plea agreement, espionage charges initially filed against Smith were dropped, and he pleaded guilty in U.S. District Court to stealing government property and assaulting a federal officer.

The FBI said Smith admitted stealing computer disks from the first officer's desk and fighting with crewmembers after he was caught. FBI agents found 17 computer disks in his possession, and a search of Smith's stateroom turned up other confidential documents related to the handling of torpedoes on Navy ships. Overindulging in alcohol may have contributed to Smith's action.

The Naval Criminal Investigative Service Field Office in Puget Sound, Washington, reported that Smith was sentenced to 260 days confinement (time served) and released on 22 December 2000.

Waguespack Leaves NACIC

Michael J. Waguespack, the National Counterintelligence Center's (NACIC) first and only Director since 1994, completed his assignment in late January 2000. During his tenure, Waguespack was the recipient of the Director of Central Intelligence's National Intelligence Medal of Achievement. On his departure, he was presented the prestigious Donovan Award by the CIA's Deputy Director of Operations, Jim Pavitt, in recognition of his contributions to the NACIC and the counterintelligence community.

He returned to FBI Headquarters where he was assigned as the Deputy Assistant Director for Counterintelligence Operations and Support, National Security Division. He remained in this position until 26 June 2001 when he was appointed Director of Counterintelligence at the Department of Energy. He replaced Ed Curran who had retired as CI Director at the end of 2000.

Jolene Hilda Neat Rector and Steven Michael Snyder

On 15 March 2001, Jolene Hilda Neat Rector and Steven Michael Snyder entered guilty pleas to a two-count indictment charging conspiracy to convey trade secrets and conveying trade secrets.

Before 20 August 1999, Rector obtained numerous pieces of proprietary information owned by R. P. Scherer, Inc. (RPS) from a friend(s) in Florida. This information included gel formulas, fill formulas, shell weights, and experimental production order data. The defendant knew that the data comprised proprietary information and trade secrets of RPS.

RPS is a leading international developer and manufacturer of drug, supplement, cosmetic, and recreational product delivery systems. RPS's proprietary advanced drug delivery systems improve the efficacy of drugs by regulating their dosage, rate of absorption, and place of release. RPS customers include global and regional manufacturers of prescription and over-the-counter pharmaceutical products, nutritional supplements, cosmetics, and recreational products such as paintballs. RPS products are produced for and placed in interstate and foreign commerce.

Sometime between 1 August and 20 August 1999, Rector requested her friend Steven Michael Snyder—then working for RPS—to send to her in Nevada the proprietary information that he had obtained from RPS. Snyder sent this information by mail, specifically including numerous experimental production orders, after Rector indicated she would use it to assist her in her current job with a competitor of RPS located in Nevada.

On 20 August 1999, Rector had a conversation with the Production Manager of Nelson Paintball, Inc. (NPB), located in Kingsford, Michigan. Rector advised him she had gelatin formulas that she wanted to sell for $50,000. Rector stated that she had obtained the formulas while working at RPS in St. Petersburg, Florida. She also stated that she

was living in Nevada, had been working for Soft Gelcaps West (SGW), and had recently been fired. Rector said that she had worked in the paintball plant and in the nutritional plant at SGW. After the conversation, the Production Manager contacted NPB's Executive Vice President regarding Rector's phone call.

On 23 August 1999, NPB's Executive Vice President received a phone call from Rector who confirmed the previous information pertaining to the formulas and, in addition, made a number of informational statements. She told the Executive Vice President that she had 65 paintball color formulas and 108 gelatin formulas belonging to RPS that she wanted to sell them for $50,000. The NPB Executive Vice President contacted the RPS corporate counsel office concerning Rector's information.

On 31 August 1999, the Vice President of Corporate Security for Cardinal Health (parent company of RPS) contacted the NPB Executive Vice President and asked him to contact Rector directly and have her fax a sample of the information for sale so that it could be evaluated. Following this conversation, the Executive Vice President contacted Rector and requested that she fax several of the fill and gel formulas, maintenance instructions, paintball facility layout map, and the pilot plant notebook. Approximately ten minutes later, the Executive Vice President received the requested documents.

NPB's Executive Vice President recontacted Rector to confirm receipt of the documents and then faxed what he had received to RPS. RPS then contacted the FBI, which opened an investigation on 1 September 1999. The investigation established that RPS is a Delaware corporation and a wholly owned subsidiary of Cardinal Health, Inc. Investigation further determined that Rector was employed at RPS in St. Petersburg, Florida, from April 1994 through November 1996.

On 29 September 1999, the NPB Executive Vice President initiated a consensual recorded phone call to Rector in Stagecoach, Nevada. During this phone conversation, she advised him that she had already sold part of the documentation to an unnamed buyer; however, she was still willing to sell the remaining documentation to NPB for $25,000.

The next day, in another consensual recorded phone call made by the Executive Vice President, Rector stated in response to his statement that she didn't sound like she wanted to come to Michigan, "Yeah, well on an illegal thing no . . . (laughing), because you know if I'm doing something that's not ill. not legally put down as like I'm doing a job . . . Yeah, then I'm setting myself up to get caught or whatever . . . you know wherever I go I'm setting myself up . . . but if there's a contract and a job, you know a job contract, then it's not a set up it, you know I'm basically doing a legal work . . . because it actually has . . . it doesn't have nobody's name on it, it is my stuff . . . "

When the Executive Vice President asked Rector what she had done with the information in the book from the pilot plant, she stated that they had rewritten it by hand and that she had destroyed the original book so that there were no names. Rector later stated that the company to whom she had sold the pharmaceutical formulas was also interested in buying the paintball formulas if she still had them.

Rector then said that she still had a maintenance manual for a Japanese Sankyo encapsulation machine, approximately 106 gel formulas, and about 60 paintball formulas to sell. Rector admitted that the examples she had faxed were from RPS.

On 14 October 1999, an undercover FBI agent met with Rector pretending to have been sent by NPB's Executive Vice President. This meeting was videotaped. Rector turned over a maroon, three-ring binder containing machine maintenance instructions, paintball and gel formulas, and list of shell weights. The undercover FBI agent then gave her a check in the amount of $25,000.

Immediately following the exchange, the FBI agent notified Rector that the meeting had been a sting,

and she consented to be interviewed even though she had been advised that she was not under arrest and was free to go. At this time, Rector admitted that she had received an RPS notebook from a former colleague—Steven Michael Snyder—via the US mail. Furthermore, Rector advised that she had burned a lab notebook containing experimental RPS products and notes while in Kentucky.

On 26 January 2000, Rector was arrested in Nevada subsequent to a Middle District of Florida complaint and admitted having received the RPS information via the mail from a specific individual in Florida. It was this information that she had turned over to the undercover FBI agent.

Both Rector and Snyder admit that the gel formulas, fill formulas, and experimental production orders are proprietary trade secrets of RPS—developed and used by them in the production of drug, nutrient supplement and paintball delivery systems (capsules), and as the fill material inside the capsules.

Rector and Snyder's offenses constitute the first-ever prosecution under the Economic Espionage Act of 1996 in the Middle District of Florida and are part of a growing number of nationwide prosecutions under this statute since it was enacted in October 1996. This case has national significance because it reinforces the impact Congress desired to make in limiting the damage industrial espionage causes United States companies, both here and abroad.

This case also demonstrates a situation where a competitor corporation (NPB) actively cooperated with federal authorities and the victimized corporation (RPS). Without the assistance of this competitor corporation, the successful prosecution of this case would not have been possible.

The defendants face a maximum term of ten years in prison and fines up to $250,000 for each offense.

Takashi Okamoto and Hiroaki Serizawa

On 8 May 2001, a grand jury in Cleveland, Ohio, returned a four-count indictment against Takashi Okamoto and Hiroaki Serizawa. They were charged with making false statements to the government, two counts of violating The Economic Espionage Act, and one count of Interstate Transportation of Stolen Property.

Okamoto and Serizawa met while both resided in Boston, Massachusetts, in the mid-1990s. Okamoto moved to Ohio where he gained employment with Lerner Research Institute (LRI) of the Cleveland Clinic Foundation (CCF) to conduct research into the cause and potential treatment for Alzheimer's disease in January 1997.

In January 1998, Okamoto and Serizawa, who was then employed by the Kansas University Medical Center (KUMC) in Kansas City, Kansas, began to conspire to misappropriate from the CCF certain genetic materials called Dioxyribonucleic Acid (DNA) and cell line reagents and constructs. Researchers employed by CCF, with funding provided by the CCF and the National Institutes of Health, developed these genetic materials to study the genetic cause of and possible treatment for Alzheimer's disease. Alzheimer's disease affects an estimated 4 million people in the United States alone and is the most common cause of dementia.

The indictment charges that Okamoto and Serizawa, and others known to the grand jury, provided an economic benefit and advantage to the Institute of Physical and Chemical Research (RIKEN) by giving RIKEN the DNA and cell line reagents and constructs that were misappropriated from the CCF. According to the indictment, RIKEN was a quasi-public corporation located in Saitama-Ken, Japan, which received more than 94 percent of its operational funding from the Ministry of Science and Technology of the Government of Japan. The Brain Science Institute (BSI) of RIKEN was formed in 1997 as a specific initiative of the Ministry of Science and Technology to conduct research in the area of neuroscience,

including research into the genetic cause of, and possible treatment for, Alzheimer's disease.

According to the indictment, in April 1999, RIKEN offered and Okamoto accepted a position as a neuroscience researcher to begin in the fall of 1999. The indictment charges that, on the evening of 8 July1999 to the early morning hours of 9 July 1999, Okamoto and a third co-conspirator known as Dr. A misappropriated DNA and cell line reagents and constructs from Laboratory 164, where Okamoto conducted research at the CCF.

Also during this time, the indictment charges that Okamoto and "Dr. A" destroyed, sabotaged, and caused to be destroyed and sabotaged the DNA and cell line reagents and constructs, which they did not remove from Laboratory 164 at the CCF. The indictment further charges that, on 10 July 1999, Okamoto stored four boxes containing the stolen DNA and cell line reagents and constructs at the Cleveland, Ohio, home of "Dr. B," a colleague at the CCF with whom Okamoto was residing temporarily.

On 12 July 1999, Okamoto then retrieved the boxes of stolen DNA and cell line reagents and constructs from Dr. B's home and sent them from Cleveland, Ohio, by private interstate carrier to Serizawa at Kansas City.

On 26 July 1999, defendant Okamoto resigned from his research position at CCF and, on 3 August 1999, started his research position with RIKEN in Japan. Okamoto returned to the United States and, on 16 August 1999, retrieved the stolen DNA and cell line reagents and constructs from Serizawa's laboratory at KUMC in Kansas City.

The indictment charges that, before Okamoto left for Japan, he and Serizawa filled small laboratory vials with tap water and made meaningless markings on the labels on the vials. Okamoto instructed Serizawa to provide these worthless vials to officials at the CCF in the event they came looking for the missing DNA and cell line reagents.

On 17 August 1999, Okamoto departed the United States for Japan and carried with him the stolen DNA and cell line reagents and constructs. The last overt act charged in the conspiracy was that, in September 1999, Serizawa provided materially false, fictitious, and fraudulent statements in an interview of him by FBI special agents who were investigating the theft of the DNA and cell line reagents from the CCF.

Count two charges that the defendants committed economic espionage by stealing trade secrets that were property of the CCF, specifically, 10 DNA and cell line reagents developed through the efforts and research of researchers employed and funded by the CCF and by a grant from the National Institutes of Health.

Count three charges a violation of The Economic Espionage Act against Okamoto and Serizawa for, without authorization, altering and destroying trade secrets that were the property of CCF.

The last count of the indictment charged Okamoto and Serizawa with transporting, transmitting, and transferring DNA and cell line reagents in interstate and foreign commerce.

Ana Belen Montes

On 21 September 2001, the FBI arrested Ana Belen Montes, a US citizen born 28 February 1957, on a US military installation in Nurnberg, Germany. She was charged with spying for Cuban intelligence for the past five years.

ANA BELEN MONTES

Montes graduated with a major in Foreign Affairs from the University of Virginia in 1979 and obtained a Masters Degree from the Johns Hopkins University School of Advanced International Studies in 1988. She is single and lived alone at 3039 Macomb Street, NW, apartment 20, Washington, DC. Until her arrest, Montes was employed by the Defense Intelligence Agency (DIA) as a senior intelligence analyst. She began her employment with DIA in September 1985 and since 1992 has specialized in Cuba matters. She worked at Bolling Air Force Base in Washington, DC. Prior to joining DIA, Montes worked at the Department of Justice. In 1993, she traveled to Cuba to study the Cuban military on a CIA-paid study for the Center for the Study of Intelligence.

Communication From the Cuban Intelligence Service (CuIS) to Montes via Shortwave Radio

During a court-authorized surreptitious entry into Montes's residence, conducted by the FBI on 25 May 2001, FBI agents observed a Toshiba laptop computer.[1] During the search, the agents electronically copied the laptop's hard drive. During subsequent analysis of the copied hard drive, the FBI recovered substantial text that had been deleted.

The recovered text from the laptop's hard drive included significant portions of a Spanish-language message, which when printed out with standard font comes to approximately 11 pages of text. The recovered portion of the message does not expressly indicate when it was composed. However, it instructs the message recipient to travel to "the Friendship Heights station" on "Saturday, November 23rd."

Although no date was on the message, November 23 fell on a Saturday in 1996. The FBI determined that this message was composed sometime before 23 November 1996 and entered onto Montes's laptop sometime after 5 October 1996, the date she purchased it. On the basis of its content, the message is from a CuIS officer to Montes.[2] Portions of the recovered message included the following: "You should go to the WIPE program and destroy that file according to the steps which we discussed during the contact. This is a basic step to take every time you receive a radio message or some disk."

During this same search, the agents also observed a Sony shortwave radio stored in a previously opened box on the floor of the bedroom. The agents turned on the radio to confirm that it was operable. Also found was an earpiece[3] that could be utilized with this shortwave radio, allowing the radio to be listened to more privately.

The recovered portion of the message begins with the following passage:

> *Nevertheless, I learned that you entered the code communicating that you were having problems with radio reception. The code alone covers a lot, meaning that we do not know specifically what types of difficulty you are having. Given that it's only been a few days since we began the use of new systems, let's not rule out that the problem might be related to them. In that case, I'm going to repeat the necessary steps to take in order to retrieve a message.*

The message then describes how the person reading the message should "write the information you send to us and the numbers of the radio messages which you receive." The message later refers to going "to a new line when you get to the group 10 of the numbers that you receive via radio," and still later gives as an "example" a series of groups of numbers: "22333 44444 77645 77647 90909 13425 76490 78399 7865498534." After some further instruction, the message states: "Here the program deciphers the message and it retrieves the text onto the screen, asking you if the text is okay or not." Near the conclusion of the message, there is the statement, "In this shipment you will receive the following disks: . . . 2) Disk 'R1' to decipher our mailings and radio."

Further FBI analysis of Montes's copied Toshiba hard drive identified text consisting of a series of 150 five-number groups. The text begins, "30107 24624" and continues until 150 such groups are listed. The FBI determined that the precise same numbers—in the precise same order—were broadcast on 6 February 1999 at AM frequency 7887 kHz, by a woman speaking Spanish, who introduced the broadcast with the words "Attencion! Attencion!" The frequency used in that February 1999 broadcast is within the frequency range of the shortwave radio observed in Montes's residence on 25 May 2001.

Communication Between the CuIS and Montes via Computer Diskette[4]

Montes communicated with her CuIS handling officer by passing and receiving computer diskettes containing encrypted messages. The message described above that was contained on the hard drive of Montes's laptop computer contained the following passage:

> *Continue writing along the same lines you have so far, but cipher the information every time you do, so that you do not leave prepared information that is not ciphered in the house. This is the most sensitive and compromising information that you hold. We realize that this entails the difficulty of not being able to revise or consult what was written previously before each shipment, but we think it is worth taking this provisional measure. It is not a problem for us if some intelligence element comes repeated or with another defect which obviously cannot help, we understand this perfectly—Give "E" only the ciphered disks. Do not give, for the time being, printed or photographed material. Keep the materials which you can justify keeping until we agree that you can deliver them.—Keep up the measure of formatting the disks we send you with couriers or letters as soon as possible, leaving conventional notes as reminders only of those things to reply to or report.*

The message goes on to refer to a "shipment" that contains "Disk 'S1'—to cipher the information you send," and, as indicated in the previous section, to "Disk 'R1' to decipher our mailings and radio." Earlier in the message, there is a reference to "information you receive either via radio or disk."

During the court-authorized search of the residence on 25 May 2001, two boxes containing a total of 16 diskettes were observed. During a subsequent search on 8 August 2001, a box containing 41 diskettes, later determined to be blank, were observed. Finally, records obtained from a Radio Shack store located near Montes's residence indicated that Montes purchased 160 floppy diskettes during the period 1 May 1993 to 2 November 1997.

Communication From Montes to the CuIS by Pager[5]

On the basis of the evidence, Montes communicated with her handling CuIS officer using a pager. In the same message copied from Montes's hard drive, there is a passage that states:

> *Beepers that you have. The only beepers in use at present are the following: 1) (917) [first seven-digit telephone number omitted from this application], use it with identification code 635. 2) (917) [second seven-digit telephone*

number omitted from this application]. Use it with identification code 937. 3) (917) [third seven-digit telephone number omitted from this application] Use it only with identification code 2900 . . . because this beeper is public, in other words it is known to belong to the Cuban Mission at the UN and we assume there is some control over it. You may use this beeper only in the event you cannot communicate with those mentioned in 1) and 2), which are secure.

The reference to "control over it" in the above passage refers to the CuIS officer's suspicion that the FBI is aware that this beeper number is associated with the Cuban Government and is monitoring it in some fashion.

In addition, the message on the laptop's hard drive includes a portion stating that the message recipient "entered the code communicating that you were having problems with radio reception." This portion of the message indicates that Montes at some point shortly prior to receiving the message sent a page to her CuIS officer handler consisting of a preassigned series of numbers to indicate she was having communication problems.

Montes's Transmission of Classified Information to the CuIS

The same message described above, as well as other messages recovered from the laptop's hard drive, contained the following information indicating that Montes had been tasked to provide and did provide classified information to the CuIS. In one portion of the message discussed above, the CuIS officer states:

*What ***[6] said during the meeting . . . was very interesting. Surely you remember well his plans and expectations when he was coming here. If I remember right, on that occasion, we told you how tremendously useful the information you gave us from the meetings with him resulted, and how we were waiting here for him with open arms.*

The very next section in the message states:

We think the opportunity you will have to participate in the ACOM exercise in December is very good. Practically, everything that takes place there will be of intelligence value. Let's see if it deals with contingency plans and specific targets in Cuba, which are to prioritized interests for us.

The "ACOM exercise in December" is a reference to a war games exercise in December 1996 conducted by the US Atlantic Command—a US Department of Defense unified command, in Norfolk, Virginia. Details about the exercise's "contingency plans and specific targets" is classified Secret and relates to the national defense of the United States. DIA advised that Montes attended the above exercise in Norfolk as part of her official DIA duties.

A separate message partially recovered from the hard drive of Montes's Toshiba laptop revealed details about a particular Special Access Program (SAP) related to the national defense of the United States:

In addition, just today the agency made me enter into a program, "special access top secret. [First name and last name omitted from this application] and I are the only ones in my office who know about the program." [The details related about this SAP in this message are classified "Top Secret" / SCI.]

DIA has confirmed that Montes and a colleague with the same name as that related in the portion of the message described above were briefed into this SAP on 15 May 1997.

In yet another message recovered from the laptop, there is a statement revealing that "we have noticed" the location, number, and type of certain Cuban military weapons in Cuba. This information is precisely the type of information that was within Montes's area of expertise and was,

in fact, an accurate statement of the US Intelligence Community's knowledge on this particular issue. The information is classified Secret.

FBI Physical Surveillance of Montes and Telephone Records for May to September 2001

The FBI maintained periodic physical surveillance of Montes during the period May to September 2001. On 20 May 2001, Montes left her residence and drove to the Hecht's on Wisconsin Avenue, in Chevy Chase, Maryland. She entered the store at 1:07 p.m. and exited by the rear entrance at 1:27 p.m. She then sat down on a stonewall outside the rear entrance and waited for approximately two minutes. At 1:30 p.m., the FBI observed her walk to a pay phone approximately 20 feet from where she was sitting. She placed a one-minute call to a pager number using a prepaid calling card. At 1:45 p.m., she drove out of the Hecht's lot and headed north on Wisconsin Avenue toward Bethesda, Maryland. At 1:52 p.m., she parked her car in a lot and went into Modell's Sporting Goods store. She quickly exited the store carrying a bag and crossed Wisconsin Avenue to an Exxon station.

She was observed looking over her right and left shoulders as she crossed the Exxon lot. At 2:00 p.m., she placed a one-minute call from a pay phone at the Exxon station to the same pager number using the same prepaid calling card. By 2:08 p.m., Montes had walked back to her vehicle and was driving back to her residence where she arrived at 2:30 p.m.

On 3 June 2001, Montes engaged in similar communications activity. She left her residence at approximately 2:30 p.m. and drove to a bank parking lot at the corner of Harrison Street, NW and Wisconsin Avenue, NW. She exited her car at approximately 2:37 p.m. and entered a Borders books store on Wisconsin Avenue. She left the store approximately 40 minutes later. She then crossed Wisconsin Avenue to the vicinity of three public pay phones near the southern exit of the Friendship Heights Metro Station. At 3:28 p.m., she placed a one-minute call using the same prepaid calling card to the same pager number she had called on 20 May 2001. After a few minutes, she walked back to her car and drove to a grocery store.

Pursuant to court authorization, on 16 August 2001, the FBI searched Montes's pocketbook. In a separate compartment of Montes's wallet, the FBI found the prepaid calling card used to place the calls on 20 May 2001 and 3 June 2001. In the same small compartment, the FBI located a slip of paper on which was written the pager number she had called. Written above this pager number was a set of digits, which comprised one or more codes for Montes to use after calling the pager number; for example, after contacting the pager, she keys in a code to be sent to the pager which communicates a particular pre-established message.

On 26 August 2001, at approximately 10:00 a.m., the FBI observed Montes making a brief pay telephone call to the same pager number from a gas station/convenience store located at the intersection of Connecticut and Nebraska Avenues, NW in Washington, DC.

On September 14, 2001, Montes left work and drove directly to her residence. She then walked to Connecticut Avenue, NW, in Washington, DC., still wearing her business clothes, and made a stop at a drycleaning shop. She then entered the National Zoo through the Connecticut Avenue entrance. She proceeded to the "Prairie Land" overlook where she stayed for only 30 seconds. She then walked further into the zoo compound and basically retraced her route out of the zoo. At approximately 6:30 p.m., Montes removed a small piece of paper or card from her wallet and walked to a public phone booth located just outside the pedestrian entrance to the zoo. Montes then made what telephone records confirmed to be two calls to the same pager number she had called in May, June, and August, as described above. The records reflect that the first call was unsuccessful—the call lasted zero seconds. According to the records, she made a second call one minute later that lasted 33 seconds. Shortly after making these calls, Montes looked at her watch and then proceeded to walk back to her residence.

On 15 September 2001, telephone records pertaining to the prepaid calling card number on the card observed in her pocketbook on 16 August 2001 showed that Montes made a call to the same pager number at 11:12 a.m. that lasted one minute.

The next day—16 September—Montes left her residence in the early afternoon and took the Metro (Red Line) to the Van Ness-UDC station in Washington, DC. She made a brief telephone call from a payphone in the Metro station at approximately 1:50 p.m., again to the same pager number.

Montes owned a cell phone, which was observed during a court-authorized search of her tote bag on 16 August 2001. In addition, during surveillance on 16 September 2001, Montes was observed speaking on a cell phone. Furthermore, telephone records obtained in May 2001 confirm that she has subscribed to cell telephone service continually from 26 October 1996 to 14 May 2001. Montes's use of public pay phones notwithstanding her access to a cell phone supports the conclusion that the pay phone calls were in furtherance of Montes's espionage.

On 19 March 2002, Montes pleaded guilty to espionage in U.S. District Court in Washington, DC, and admitted that, for 16 years, she had passed top secret information to Cuban intelligence. She used shortwave radios, encrypted transmissions, and a pay telephone to contact Cuban intelligence officials and provide them the names of four US intelligence officers working in Cuba. She also informed Cuban intelligence about a US "special access program" and revealed that the US Government had uncovered the location of various Cuban military installations.

Both her defense attorney and federal prosecutors said that Montes was motivated by her moral outrage at US policy toward Cuba—an impoverished island country—and not by money. She received only "nominal" expenses for her activities.

Although Montes could receive the death penalty for her crime, the plea agreement calls for a 25-year prison term if she cooperates with the FBI and other investigators by providing all the details she knows about Cuban intelligence activities. Judge Ricardo M. Urbina set a sentencing date of September 2002.

Endnotes

[1] A receipt obtained from a CompUSA store located in Alexandria, Virginia, indicated that, on 5 October 1996, one "Ana B. Montes" purchased a refurbished Toshiba laptop computer, model 405CS, serial number 10568512. The Toshiba laptop in her apartment had the same serial number on it as the one she purchased.

[2] The CuIS often communicates with clandestine CuIS agents operating outside Cuba by broadcasting encrypted messages at certain high frequencies. Under this method, the CuIS broadcasts a series of numbers on a particular frequency. The clandestine agent, monitoring the message on a shortwave radio, keys in the numbers onto a computer and then uses a diskette containing a decryption program to convert the seemingly random series of numbers into Spanish-language text. This was the methodology employed by some of the defendants convicted last June in the Southern District of Florida of espionage on behalf of Cuba and acting as unregistered agents of Cuba, in the case of United States of America v. Gerardo Hernandez, et al. (See Cuban Spies in Miami). Although it is very difficult to decrypt a message without access to the relevant decryption program, once decrypted on the agent's computer the decrypted message resides on the computer's hard drive unless the agent takes careful steps to cleanse the hard drive of the message. Simply "deleting" the file is not sufficient.

[3] Similar earpieces were found in the residences of the defendants in the Hernandez case.

[4] On the basis of knowledge of the methodology employed by the CuIS, a clandestine CuIS agent often communicates with his or her handling CuIS officer by typing a message onto a computer and then encrypting and saving it to a diskette. The agent, thereafter, physically delivers the diskette, either directly or indirectly, to the officer. In addition, as an alternative to sending an encrypted shortwave radio broadcast, a CuIS officer often will similarly place an encrypted message

onto a diskette and again simply physically deliver the diskette, clandestinely, to the agent. Upon receipt of the encrypted message, either by the CuIS officer or the agent, the recipient employs a decryption program contained on a separate diskette to decrypt the message. The exchange of diskettes containing encrypted messages, and the use of decryption programs contained on separate diskettes, was one of the clandestine communication techniques utilized by the defendants in the Hernandez case. Although it is difficult to decrypt a message without the decryption program, the very process of encrypting or decrypting a message on a computer causes a decrypted copy of the message to be placed on the computer's hard drive. Unless affirmative steps are taken to cleanse the hard drive—beyond simply "deleting" the message—the message can be retrieved from the hard drive.

[5] On the basis of knowledge of the methodology employed by the CuIS, a clandestine CuIS agent often communicates with his or her handling CuIS officer by making calls to a pager number from a pay telephone booth and entering a preassigned code to convey a particular message. The defendants in the Hernandez case also utilized this methodology.

[6] The FBI replaced in this application with "***" a word that begins with a capital letter, which was not translated, and is, in fact, the true last name of a US intelligence officer who was present in an undercover capacity, in Cuba, during a period that began prior to October 1996. The above quoted portion of the message indicates that Montes disclosed the US officer's intelligence agency affiliation and anticipated presence in Cuba to the CuIS, which information is classified "Secret." As a result, the Cuban Government was able to direct its counterintelligence resources against the US officer ("we were waiting here for him with open arms").

The Threat to Laptop Computers

The greatest threat to laptop computers comes from common thieves. A laptop is valuable, compact, very transportable, and relatively easy to steal in a public place. Police have noted that, in terms of attractiveness to criminals and their customers who purchase stolen goods, the laptop is the equivalent of the VCR and offers criminals the opportunity to exploit a whole new market—putting it at a much higher risk than the VCR that stayed at home.

A survey of 643 major corporations conducted in 2000 by the FBI and the San Francisco–based Computer Science Institute found that 60 percent of these corporations have suffered laptop thefts. Overall, nearly 320,000 laptops were stolen in the United States in 1999. According to Safeware, a computer insurance firm in Columbus, Ohio, 309,000 laptop computers were stolen in the United States during 1997—up from 208,000 in 1995—and 10 percent of all laptop thefts occurred in airports. Only virus attacks are a more prevalent security problem.

Thieves take advantage of airport hustle to steal laptops. One scam has a female accomplice tap an unsuspecting traveler on the shoulder. "You have ketchup on your shoulder," she tells him, while handing him a tissue. The traveler puts down his laptop and dabs the messy condiment off his jacket. While he is distracted, the accomplice walks off with the laptop.

In another example, a consultant on a large project employing about a hundred other consultants traveled in and out of the same airport every weekend. Each consultant was issued the same company laptop and the same computer bag. On one occasion, the consultant believed that someone tried to switch computer bags with him but that the other individual's bag was not heavy enough to contain a computer. When the consultant yelled at the individual, he acted confused, said he was sorry, and returned the consultant's bag.

Throughout Europe, laptops are also a prime target for theft. International travelers who anticipate carrying such items should be particularly wary while transiting airports. Airports offer a particularly inviting atmosphere for laptop thieves because of large crowds, hectic schedules, and weary travelers. Laptop thefts commonly occur in places where people set them down—at security checkpoints, pay phones, lounges and restaurants, check-in lines, and restrooms.

Incidents at separate European airports demonstrate the modus operandi of thieves operating in pairs to target laptops. In the first incident, Brussels International Airport security reported that two thieves exploited a contrived delay around the security X-ray machines. The first thief preceded the traveler through the security checkpoint and then loitered around the area where security examines carry-on luggage. When the traveler placed his laptop onto the conveyer belt of the X-ray machine, the second thief stepped in front of the traveler and set off the metal detector. With the traveler now delayed, the first thief removed the traveler's laptop from the conveyer belt just after it passed through the X-ray machine and quickly disappeared.

In the second incident, a traveler walking around Frankfurt International Airport in Germany and carrying a laptop in his roll bag did not realize that a thief was walking in front of him. The thief stopped abruptly as the traveler bypassed a crowd of people, causing the traveler to also stop. A second thief, who was following close behind, quickly removed the traveler's laptop computer from his roll bag and disappeared into the crowd.

A traveler to Russia may have his laptop confiscated by the Russian Government. In 1998, two US Government contractors, working on a joint US-Russian project, had completed their task and were returning home. As they passed through Russian Customs, the official told one of the contractors that they would have to surrender their laptops to Russian authorities. When the contractors protested, the Russian official said that Russian law requires the laptop computers to be examined 48 hours before leaving the country to determine if any Russian "secrets" were being smuggled out of the country. This is the only time of which the US Government is aware that the Russians have used a catchall paragraph in their law to retain a laptop. Letters were sent requesting the return of the laptops, and they were returned six months later.

At Orly Airport in Paris, a US Government contractor had his laptop stolen from an airport bus as he was transferring from one airport gate to another after a change in his flight. The contractor had taken all precautions to guard his laptop while in France until he boarded the bus. Thinking he was safe, he placed his laptop with his other bags on the luggage rack. When he went to retrieve it, the laptop was gone.

In late October 2000, Julien Holstein, information security director at Airbus, warned travelers not to work on company-sensitive projects on laptop computers while flying. During his talk at the Computer Security, Audit, and Control conference in London, Holstein said his firm introduced a companywide policy forbidding Airbus staff to work on projects using their laptops when flying on business. The policy had been introduced "to maintain the integrity of the company's data after one of its managers reported that he had covertly read sensitive project information off the laptop screen of the person in the next seat."[1]

At the Department of State, a laptop that contained thousands of pages of highly classified information disappeared on 20 January 2000 from an allegedly secure workspace in the Office of Strategic Proliferation and Military Affairs in the Bureau of Intelligence and Research. It has yet to be recovered. An inventory at State Department headquarters in Washington confirmed that 15 out of 1,913 unclassified laptop computers are missing. "It's possible they were stolen," a spokesman said. "Some could be lost." Only one classified computer is missing so far, and department officials still aren't sure if espionage was involved.

The FBI is investigating whether the theft of a laptop owned by Qualcomm's CEO Irwin Jacobs was the work of thieves or an act of economic espionage. After speaking to members of the Society of American Business Editors and Writers at the Hyatt-Regency in Irvine, California, in September 2000, the CEO went over to speak to a small group of attendees. When he returned 15 to 20 minutes later, his IBM Think-Pad laptop—worth about $4,000—was gone. The CEO said that the laptop contained proprietary information that could be valuable to foreign governments.

The FBI is not exempt from losing laptops. Conducting an internal inventory, the FBI discovered that 184 laptop computers, including at least one containing classified data, were missing or perhaps stolen. The secret data on the laptop concerned two closed cases. Bureau officials also said three other missing computers were suspected of containing classified information.

The loss of classified US Government information and US proprietary information is not limited to laptop thefts in the United States. In Canada, Ottawa businesses and institutions reported that $6.7 million of computer equipment was stolen in 1997.[2]

In May 2000, a laptop was taken from a British naval intelligence officer as he sat on a train at London's Paddington Station. The laptop contained top secret information on the supersonic Anglo-US Strikefighter. After being stolen, the computer passed through a number of hands. It came into *The Mirror*'s (a British newspaper) possession after a computer specialist who said that a contact wanted him to wipe a laptop of "fighter plane stuff" contacted the paper. *The Mirror*, which bought a new machine and switched laptops without the original contact being aware, returned the laptop to the British Government. A relieved military expert said, "It is unbelievable it could be stolen apparently so easily."

The above laptop was stolen from the same rail station where, two months previously, an MI5 officer (British internal security service) had his laptop stolen when he put it down to buy a ticket. Just a few days later, a laptop was mislaid by an MI6 (British foreign intelligence) officer who had been drinking at a tapas bar near MI6's South London headquarters. It is thought that he left it in a taxi on the way home. The officer did not realize it was missing until the next day. In April 1999, an Army officer had a laptop stolen at Heathrow Airport. A portable PC belonging to a British Royal Navy Commander was later taken from a car in Pinner, Middlesex. The computer, which contained top secret and classified material, was not password protected.

It appears that British media coverage of missing laptops has had no real affect on security practices because in April 2001 another British Ministry of Defense (MoD) official left his laptop containing top secret information in a taxi. According to the British press, the individual reported the missing laptop to the police station in Wandsworth, South London. The official informed the police that he had taken a cab near Waterloo railway station to Roehampton. When he got out of the taxi, he forgot about the laptop and left it in the cab. Police immediately alerted Scotland Yard's Special Branch. This is only the latest of a large number of computers that have gone missing through carelessness or theft—sometimes after drinking sessions

The Mirror reported that, since 1997, military and intelligence staffs have lost an astonishing 204 laptops containing official secrets. The problem is so serious that the MoD and security service staffs are to be issued hi-tech briefcases costing 1,000 pounds each. The MoD plans to buy 15,000 of the armoured cases that look like ordinary black briefcases but will destroy data if an unauthorized attempt is made to open them.

The Mirror, citing an MoD spokesperson, stated that the new briefcases are so strong that they can withstand a Semtex explosion. Special versions will have an electronic system that erases the laptop's hard drive if the case is opened without the right codes. The briefcases were recently displayed at a private security exhibition at the

MoD's Whitehall headquarters and were passed for use by a secretive Cabinet Office body called the Security Equipment Assessment Panel. Some of the briefcases will also be fitted with electronic trackers so that they can be traced quickly if they are misplaced.[3]

If your company's security is not adequate, thieves can enter your office and steal proprietary information. Consider the case of John Labatt Ltd., whose offices were entered by a thief who stole five laptop computers. The physical security at Labatt in the heart of Toronto's financial district was easily breached. Espionage is suspected because the thief ignored cash and other valuables. Labatt is being eyed by at least two suitors for a hostile takeover so that any private information would be of much greater value on the street than just the physical worth of the laptops.

A laptop is not immune from theft in a hotel. Some countries convince hotel operators to provide intelligence collectors with access to visitors' luggage or rooms. During these surreptitious break-ins, known colloquially as "bag ops," unattended luggage is searched for sensitive information, and any useful documents are copied or simply stolen.

Economic and industrial espionage may involve simply breaking into a hotel room or an office containing desired information. Break-ins at the foreign offices of American companies have resulted in the theft of laptop computers and/or disks even when more valuable items are in the vicinity. These instances are not always reported, or they are reported as merely break-ins, without considering the possibility that the target was information rather than equipment.

In another example, a major US consumer products company suffered a possible loss of proprietary information as a result of a theft in East Asia. A laptop computer containing sales data, market estimates, and strategic business plans for one of its business units was stolen from a hotel conference room during a lunch break. Hotel staff—under the supervision of a company employee who was preparing remarks for the next presentation—cleaned the room for the afternoon session. The employee did not continuously guard the computer and discovered the loss shortly before the session reconvened.

When a laptop is stolen, one doesn't know whether it was taken for the value of the information on the computer or for the value of the computer itself. This makes it difficult to assess the damage caused by the loss. In addition, stolen laptops are rarely recovered mainly because it is difficult to prove ownership if the owner did not bother to record the laptop's serial number.

Endnotes

[1] Lynch, Ian. "Laptop secrets not safe on planes." NewMonday.com, 3 November 2000.

[2] *Monitor Magazine*, April 1997.

[3] "The Laptop Shambles." *The Mirror*, 16 April 2001.

The Presidential Decision Directive on CI-21: Counterintelligence for the 21st Century

The White House released the following on 6 January 2001:

FACT SHEET

President Clinton signed a Presidential Decision Directive (PDD) entitled "U.S. Counterintelligence Effectiveness—Counterintelligence for the 21st Century." The PDD outlines specific steps that will enable the U.S. counterintelligence (CI) community to better fulfill its mission of identifying, understanding, prioritizing and counteracting the intelligence threats faced by the United States. The system will be predictive, proactive and will provide integrated oversight of counterintelligence issues across the national security agencies.

Specifically, the PDD directs the following structure be established to continue the task of improving U.S. counterintelligence effectiveness:

Counterintelligence Board of Directors

- A National Counterintelligence Board of Directors, chaired by the Director, FBI and composed of the Deputy Secretary of Defense, Deputy Director of Central Intelligence and a senior representative of the Department of Justice is hereby established.

- The Board, chaired by the Director of the FBI, will operate by consensus, and will select, oversee and evaluate the National Counterintelligence Executive (CI Executive) and will promulgate the mission, role and responsibilities of the CI Executive.

- The Board will approve the National Counterintelligence Strategy drawn from the annual National Threat Identification and Prioritization Assessment, ensuring the integration of government and private sector interests.

- The Board working with Congress, OMB, and other Executive Branch agencies will ensure the CI Executive has adequate resources to carry out his/her responsibilities and duties.

NSC Deputies Committee

- The NSC Deputies Committee, to include the Director of the FBI, will review the annual National Threat Identification and Prioritization Assessment and will meet at least semiannually, to review progress in implementing the National Counterintelligence Strategy.

- The Deputies Committee will ensure that the strategy, priorities and activities of the CI Community are grounded in national policy goals and objectives; the Deputies Committee shall also ensure that CI analysis and information is provided to assist national policy deliberations as appropriate. The Board of Directors through the CI Executive will be responsible for ensuring the implementation of these decisions.

The National Counterintelligence Executive

- The position of CI Executive is established and empowered to execute certain responsibilities on behalf of the Board of Directors and will serve as the substantive leader of national-level counterintelligence. The CI Executive will be a federal employee, selected by the Board of Directors with the concurrence of the Attorney General, DCI and the Secretary of Defense.

- The CI Executive will report to the FBI Director, as Chairman of the Board of Directors, but will be responsible to the Board of Directors as a whole. The Board will, through the Chairman, oversee and evaluate the CI Executive.

- The CI Executive and the National Coordinator for Security, Infrastructure Protection and Counterterrorism will work together to insure that both of their programs are well coordinated with each other.

- The CI Executive, in carrying out the duties and responsibilities of the position, will advise members of the Board on counterintelligence programs and policies.

The National Counterintelligence Policy Board

- The CI Executive will chair the National Counterintelligence Policy Board. Senior counterintelligence officials from State, Defense, Justice, Energy, JCS, CIA, FBI and NSC Staff, at a minimum will serve on the Policy Board. The NSC Deputies Committee will approve the composition, functions and duties of the Policy Board, which will be consistent with the statutorily defined functions of the Policy Board. The Policy Board will establish, with the approval of the Board of Directors, other interagency boards and working groups as necessary.

- The Policy Board, under the chairmanship of the CI Executive, will serve as an Interagency Working Group to prepare issues relating to the full implementation of this PDD for Deputies discussions and review, as well as a forum to provide advice to the CI Executive on priorities with respect to the National Counterintelligence Strategy.

Office of the CI Executive

- The CI Executive, on behalf of the Board of Directors, will head the Office of the National Counterintelligence Executive, which will among its other functions assume the functions previously exercised by the NACIC. To the extent permitted by law, resources previously assigned to the NACIC will become the initial resource base for the Office of the CI Executive. The Office will develop and deploy the following capabilities:

National CI Strategic Planning

- The Office, in consultation with United States government agencies and the private sector, will produce an annual report entitled The National Threat Identification and Prioritization Assessment for review by the Deputies Committee.

- The Office, drawing on this Assessment and working with the policy community, appropriate Government counterintelligence organizations and the private sector, will formulate and, subject to the approval of the Board of Directors, publish the National Counterintelligence Strategy.

National CI Strategic Analysis

- The Office will oversee and coordinate the production of strategic national CI analysis and will be supported in this endeavor by all components of the Executive Branch.

- The Office will oversee and coordinate the production of CI damage assessments and "lessons learned" papers with full support from Executive Branch components.

National CI Program Budget and Evaluation

- The Office, working with the DCI's Community Management Staff, will review, evaluate, and coordinate the integration of CI budget and resource plans of, initially, the DOD, CIA and FBI. It will report to the Board of Directors and the Deputies Committee on how those plans meet the objectives and priorities of the National CI Strategy.

- The Office will evaluate the implementation of the National CI Strategy by the CI community agencies and report to the Board of Directors and Deputies Committee. The Office will also identify shortfalls, gaps and weaknesses in agency programs and recommend remedies.

National CI Collection and Targeting Coordination

- The Office will develop for approval by the Board of Directors strategic CI investigative, operational and collection objectives and priorities that implement the National CI Strategy.

- The Office will not have an operational role in CI operations and investigations and no independent contacts or activities with foreign intelligence services.

National CI Outreach, Watch and Warning Capability

- The Office will conduct and coordinate CI vulnerability surveys throughout government, and with the private sector as appropriate, while working with the Security Policy community. It will engage government and private sector entities to identify more clearly and completely what must be protected.

- The Office will conduct and coordinate CI community outreach programs in the government and private sector. It will serve as the national coordination mechanism for issuing warnings of counterintelligence threats to the national security.

- The Office will work with various government and private sector R&D centers to explore technology needs and solutions for the CI community. The Office will ensure that emerging technology and products and services are used effectively.

In addition, the Office will develop policies for CI training and professional development for CI investigators, operators, and analysts. It will also develop and manage joint training exercises, and assess the need for a National CI Training Academy. Also, the CI Executive and the Office will have a Principal Legal Advisor who will ensure that all activities of the Executive and the office comport with the law, Executive Orders and Attorney General Guidelines. The Principal Legal Advisor will provide advice and counsel to the Executive and the Office regarding national security law issues. The Advisor will coordinate with the appropriate law enforcement, intelligence and defense agencies' General Counsels and Legal Advisors in providing legal advice, guidance and representation to the Executive and the Office.

National Security Presidential Directive-1

(*Editor's Note: President George W. Bush decided that the directives used to promulgate Presidential decisions on national security matters would be designated National Security Presidential Directives [NSPDs]. This new category of directives supersedes both the Presidential Decision Directives and the Presidential Review Directives of the Clinton Administration.*)

SUBJECT: Organization of the National Security Council System

This document is the first in a series of National Security Presidential Directives. National Security Presidential Directives shall replace both Presidential Decision Directives and Presidential Review Directives as an instrument for communicating presidential decisions about the national security policies of the United States.

National security includes the defense of the United States of America, protection of our constitutional system of government, and the advancement of United States interests around the globe. National security also depends on America's opportunity to prosper in the world economy. The National Security Act of 1947, as amended, established the National Security Council to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. That remains its purpose. The NSC shall advise and assist me in integrating all aspects of national security policy as it affects the United States - domestic, foreign, military, intelligence, and economics (in conjunction with the National Economic Council (NEC)). The National Security Council system is a process to coordinate executive departments and agencies in the effective development and implementation of those national security policies.

The National Security Council (NSC) shall have as its regular attendees (both statutory and non-statutory) the President, the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the Assistant to the President for National Security Affairs. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff, as statutory advisors to the NSC, shall also attend NSC meetings. The Chief of Staff to the President and the Assistant to the President for Economic Policy are invited to attend any NSC meeting. The Counsel to the President shall be consulted regarding the agenda of NSC meetings, and shall attend any meeting when, in consultation with the Assistant to the President for National Security Affairs, he deems it appropriate. The Attorney General and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities. For the Attorney General, this includes both those matters within the Justice Department's jurisdiction and those matters implicating the Attorney General's responsibility under 28 U.S.C. 511 to give his advice and opinion on questions of law when required by the President. The heads of other executive departments and agencies, as well as other senior officials, shall be invited to attend meetings of the NSC when appropriate.

The NSC shall meet at my direction. When I am absent from a meeting of the NSC, at my direction the Vice President may preside. The Assistant to the President for National Security Affairs shall be responsible, at my direction and in consultation with the other regular attendees of the NSC, for determining the agenda, ensuring that necessary papers are prepared, and recording NSC actions and Presidential decisions. When international economic issues are on the agenda of the NSC, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy shall perform these tasks in concert.

The NSC Principals Committee (NSC/PC) will continue to be the senior interagency forum for consideration of policy issues affecting national security, as it has since 1989. The NSC/PC shall have as its regular attendees the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Chief of Staff to the President, and the Assistant to the President for National Security Affairs (who shall serve as chair). The Director

of Central Intelligence and the Chairman of the Joint Chiefs of Staff shall attend where issues pertaining to their responsibilities and expertise are to be discussed. The Attorney General and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities. For the Attorney General, this includes both those matters within the Justice Department's jurisdiction and those matters implicating the Attorney General's responsibility under 28 U.S.C. 511 to give his advice and opinion on questions of law when required by the President. The Counsel to the President shall be consulted regarding the agenda of NSC/PC meetings, and shall attend any meeting when, in consultation with the Assistant to the President for National Security Affairs, he deems it appropriate. When international economic issues are on the agenda of the NSC/PC, the Committee's regular attendees will include the Secretary of Commerce, the United States Trade Representative, the Assistant to the President for Economic Policy (who shall serve as chair for agenda items that principally pertain to international economics), and, when the issues pertain to her responsibilities, the Secretary of Agriculture. The Chief of Staff and National Security Adviser to the Vice President shall attend all meetings of the NSC/PC, as shall the Assistant to the President and Deputy National Security Advisor (who shall serve as Executive Secretary of the NSC/PC). Other heads of departments and agencies, along with additional senior officials, shall be invited where appropriate.

The NSC/PC shall meet at the call of the Assistant to the President for National Security Affairs, in consultation with the regular attendees of the NSC/PC. The Assistant to the President for National Security Affairs shall determine the agenda in consultation with the foregoing, and ensure that necessary papers are prepared. When international economic issues are on the agenda of the NSC/PC, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy shall perform these tasks in concert.

The NSC Deputies Committee (NSC/DC) will also continue to serve as the senior sub-Cabinet interagency forum for consideration of policy issues affecting national security. The NSC/DC can prescribe and review the work of the NSC interagency groups discussed later in this directive. The NSC/DC shall also help ensure that issues being brought before the NSC/PC or the NSC have been properly analyzed and prepared for decision. The NSC/DC shall have as its regular members the Deputy Secretary of State or Under Secretary of the Treasury or Under Secretary of the Treasury for International Affairs, the Deputy Secretary of Defense or Under Secretary of Defense for Policy, the Deputy Attorney General, the Deputy Director of the Office of Management and Budget, the Deputy Director of Central Intelligence, the Vice Chairman of the Joint Chiefs of Staff, the Deputy Chief of Staff to the President for Policy, the Chief of Staff and National Security Adviser to the Vice President, the Deputy Assistant to the President for International Economic Affairs, and the Assistant to the President and Deputy National Security Advisor (who shall serve as chair). When international economic issues are on the agenda, the NSC/DC's regular membership will include the Deputy Secretary of Commerce, a Deputy United States Trade Representative, and, when the issues pertain to his responsibilities, the Deputy Secretary of Agriculture, and the NSC/DC shall be chaired by the Deputy Assistant to the President for International Economic Affairs for agenda items that principally pertain to international economics. Other senior officials shall be invited where appropriate.

The NSC/DC shall meet at the call of its chair, in consultation with the other regular members of the NSC/DC. Any regular member of the NSC/DC may also request a meeting of the Committee for prompt crisis management. For all meetings the chair shall determine the agenda in consultation with the foregoing, and ensure that necessary papers are prepared.

The Vice President and I may attend any and all meetings of any entity established by or under this directive.

Management of the development and implementation of national security policies by multiple agencies of the United States Government shall usually be accomplished by the NSC Policy Coordination Committees (NSC/PCCs). The NSC/PCCs shall be the main day-to-day fora for interagency coordination of national security policy. They shall provide policy analysis for consideration by the more senior committees of the NSC system and ensure timely responses to decisions made by the President. Each NSC/PCC shall include representatives from the executive departments, offices, and agencies represented in the NSC/DC.

Six NSC/PCCs are hereby established for the following regions: Europe and Eurasia, Western Hemisphere, East Asia, South Asia, Near East and North Africa, and Africa. Each of the NSC/PCCs shall be chaired by an official of Under Secretary or Assistant Secretary rank to be designated by the Secretary of State.

Eleven NSC/PCCs are hereby also established for the following functional topics, each to be chaired by a person of Under Secretary or Assistant Secretary rank designated by the indicated authority:

Democracy, Human Rights, and International Operations (by the Assistant to the President for National Security Affairs);

International Development and Humanitarian Assistance (by the Secretary of State);

Global Environment (by the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy in concert);

International Finance (by the Secretary of the Treasury);

Transnational Economic Issues (by the Assistant to the President for Economic Policy);

Counter-Terrorism and National Preparedness (by the Assistant to the President for National Security Affairs);

Defense Strategy, Force Structure, and Planning (by the Secretary of Defense);

Arms Control (by the Assistant to the President for National Security Affairs);

Proliferation, Counterproliferation, and Homeland Defense (by the Assistant to the President for National Security Affairs);

Intelligence and Counterintelligence (by the Assistant to the President for National Security Affairs); and

Records Access and Information Security (by the Assistant to the President for National Security Affairs).

The Trade Policy Review Group (TPRG) will continue to function as an interagency coordinator of trade policy. Issues considered within the TPRG, as with the PCCs, will flow through the NSC and/or NEC process, as appropriate.

Each NSC/PCC shall also have an Executive Secretary from the staff of the NSC, to be designated by the Assistant to the President for National Security Affairs. The Executive Secretary shall assist the Chairman in scheduling the meetings of the NSC/PCC, determining the agenda, recording the actions taken and tasks assigned, and ensuring timely responses to the central policymaking committees of the NSC system. The Chairman of each NSC/PCC, in consultation with the Executive Secretary, may invite representatives of other executive departments and agencies to attend meetings of the NSC/PCC where appropriate.

The Assistant to the President for National Security Affairs, at my direction and in consultation with the Vice President and the Secretaries of State, Treasury, and Defense, may establish additional NSC/PCCs as appropriate.

The Chairman of each NSC/PCC, with the agreement of the Executive Secretary, may establish subordinate working groups to assist the PCC in the performance of its duties.

The existing system of Interagency Working Groups is abolished.

The oversight of ongoing operations assigned in PDD/NSC-56 to Executive Committees of the Deputies Committee will be performed by the appropriate regional NSC/PCCs, which may create subordinate working groups to provide coordination for ongoing operations.

The Counter-Terrorism Security Group, Critical Infrastructure Coordination Group, Weapons of Mass Destruction Preparedness, Consequences Management and Protection Group, and the interagency working group on Enduring Constitutional Government are reconstituted as various forms of the NSC/PCC on Counter-Terrorism and National Preparedness.

The duties assigned in PDD/NSC-75 to the National Counterintelligence Policy Group will be performed in the NSC/PCC on Intelligence and Counterintelligence, meeting with appropriate attendees.

The duties assigned to the Security Policy Board and other entities established in PDD/NSC-29 will be transferred to various NSC/PCCs, depending on the particular security problem being addressed.

The duties assigned in PDD/NSC-41 to the Standing Committee on Nonproliferation will be transferred to the PCC on Proliferation, Counterproliferation, and Homeland Defense.

The duties assigned in PDD/NSC-35 to the Interagency Working Group for Intelligence Priorities will be transferred to the PCC on Intelligence and Counterintelligence.

The duties of the Human Rights Treaties Interagency Working Group established in E.O. 13107 are transferred to the PCC on Democracy, Human Rights, and International Operations. The Nazi War Criminal Records Interagency Working Group established in E.O. 13110 shall be reconstituted, under the terms of that order and until its work ends in January 2002, as a Working Group of the NSC/PCC for Records Access and Information Security.

Except for those established by statute, other existing NSC interagency groups, ad hoc bodies, and executive committees are also abolished as of March 1, 2001, unless they are specifically reestablished as subordinate working groups within the new NSC system as of that date. Cabinet officers, the heads of other executive agencies, and the directors of offices within the Executive Office of the President shall advise the Assistant to the President for National Security Affairs of those specific NSC interagency groups chaired by their respective departments or agencies that are either mandated by statute or are otherwise of sufficient importance and vitality as to warrant being reestablished. In each case the Cabinet officer, agency head, or office director should describe the scope of the activities proposed for or now carried out by the interagency group, the relevant statutory mandate if any, and the particular NSC/PCC that should coordinate this work. The Trade Promotion Coordinating Committee established in E.O. 12870 shall continue its work, however, in the manner specified in that order. As to those committees expressly established in the National Security Act, the NSC/PC and/or NSC/DC shall serve as those committees and perform the functions assigned to those committees by the Act.

To further clarify responsibilities and effective accountability within the NSC system, those positions relating to foreign policy that are designated as special presidential emissaries, special envoys for the President, senior advisors to the President and the Secretary of State, and special advisors to the President and the Secretary of State are also abolished as of March 1, 2001, unless they are specifically redesignated or reestablished by the Secretary of State as positions in that Department.

This Directive shall supersede all other existing presidential guidance on the organization of the National Security Council system. With regard to application of this document to economic matters, this document shall be interpreted in concert with any Executive Order governing the National Economic Council and with presidential decision documents signed hereafter that implement either this directive or that Executive Order.

[signed: George W. Bush]

cc: The Executive Clerk

Aldrich, Richard J. *Intelligence and the War Against Japan: Britain, America and the Politics of Secret Service*. Cambridge University Press, Cambridge, UK, 2000.

Espionage, Security and Intelligence in Britain 1945-1970. Manchester University Press, Manchester, UK, 1998.

Allen, George W. *None So Blind: A Personal Account of the Intelligence Failure in Vietnam*. Ivan R. Dee, Inc., Chicago, IL, 2001.

Alvarez, David. *Secret Messages: Codebreaking and American Diplomacy: 1930-1945*. University Press of Kansas, Lawrence, KS, 2000.

Andrew, Christopher and Vasili Mitrokhin. *The Sword and The Shield: The Mitrokhin Archive and the Secret History of the KGB*. Basic Books, New York, NY, 1999.

Bath, Alan Harris. *Tracking the Axis Enemy: The Triumph of Anglo-American Naval Intelligence*. University Press of Kansas, Lawrence, KS, 1998.

Bamford, James. *Body of Secrets: Anatomy of the Ultra Secret National Security Agency*. Doubleday, New York, NY, 2001.

Beesly, Patrick. *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Centre, 1939-1945*. Greenhill Books/Lionel Levanthal, London, UK, 2000.

Berkowitz, Bruce D. and Allan E. Goodman. *Best Truth: Intelligence in the Information Age*. Yale University Press, New Haven, CT, 2000.

Budiansky, Stephen. *Battle of Wits: The Complete Story of Codebreaking in World War II*. Free Press, New York, NY, 2000.

Burrows, William E. *By Any Means Necessary: America's Secret Air War in the Cold War*. Farrar, Straus & Giroux, New York, NY, 2001.

Cole, D.S. *Geoffrey Prime: The Imperfect Spy*. Robert Hale Ltd, London, UK, 2001.

Conboy, Kenneth and Dale Andrade. *Spies and Commandos: How America Lost the Secret War in North Vietnam*. University Press of Kansas, Lawrence, KS, 2000.

Conboy, Kenneth and James Morrison. *Feet to the Fire: CIA Covert Operations in Indonesia, 1957-1958*. Naval Institute Press, Annapolis, MD, 2000.

Daugherty, William J. *In the Shadow of the Ayatollah: A CIA Hostage in Iran*. Naval Institute Press, Annapolis, MD, 2001.

Day, Dwayne A, ed. *Eye in the Sky: The Story of the Corona Spy Satellites*. Smithsonian Institution Press, Washington, D.C., 1998.

de Graffenreid, Kenneth, ed. *The Cox Report*. Regnery Publishing, Washington, DC, 1999.

Dorril, Stephen, MI: *Inside the Covert World of Her Majesty's Secret Intelligence Service*. The Free Press, New York, NY, 2000.

Doyle, David W. *True Men and Traitors: From the OSS to the CIA, My Life in the Shadows*, John Wiley & Sons, New York, NY, 2001.

Duff, William E. *A Time for Spies: Theodore Stephanovich Mally and the Era of the Great Illegals*. Vanderbilt University Press, Nashville, TN, 1999.

Douglas, Hugh. *Jacobite Spy Wars: Moles, Rogues and Treachery*. Sutton Publishing, Phoenix Mill, UK, 1999.

Eisendrath, Craig R., ed. *National Insecurity: US Intelligence After the Cold War*. Temple University Press, Philadelphia, PA, 1999.

Feklisov, Alexander and Sergei Kostin. *The Man Behind the Rosenbergs*. Enigma Books, New York, NY, 2001.

Gannon, James. *Stealing Secrets, Telling Lies: How Spies & Codebreakers Helped Shape the Twentieth Century*. Brasseys Inc., New York, NY, 2001.

Gertz, Bill. *Betrayal*. Regnery Publishing Inc., Washington, DC, 1999.

Gibson, Steve. *The Last Mission: Behind the Iron Curtain*. Sutton Publishing, Phoenix Mill, UK, 1998.

Goldenberg, Elliot and Alan Dershowitz. *The Hunting Horse: The Truth Behind the Jonathan Pollard Spy Case*. Prometheus Books, Amhurst, NY, 2000.

Golitt, Leslie. *Spy Master, The Real-Life Karla, His Moles and the East German Secret Police*. Addison-Wesley Publishing Co., Reading, MA, 1995.

Gross, Peter. *Operation Rollback: America's Secret War behind the Iron Curtain*. Houghton Mifflin Co., Boston, MA, 2000.

Gudgin, Peter. *Military Intelligence: A History*. Sutton Publishing, Phoenix Mill, UK, 2000.

Gup, Ted. *The Book of Honor Covert Lives and Classified Deaths at the CIA*. Random House, New York, NY, 2000.

Harvill, Adrian. *The Spy Who Stayed Out in the Cold: The Secret Life of FBI Double Agent Robert Hanssen*. St. Martin's Press, New York, NY, 2001.

Haynes, John Earl and Harvey Klehr. *Venona: Decoding Soviet Espionage in America*. Yale University Press, New Haven, CT, 1999.

Herrington, Stuart A. *Traitors Among US, Inside the Spy Catcher's World*. Presidio Press, Novato, CA, 1999.

Holobar, Frank. *Raiders of the China Coast*: *CIA Covert Operations during the Korean War*. Naval Institute Press, Annapolis, MD, 1999.

Hunter, Robert W. *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case*. Naval Institute Press, Annapolis, MD, 1999.

Jackson, Robert. *High Cold War: Strategic Air Reconnaissance and the Electronics Intelligence War*. Patrick Stephens Limited, Somerset, UK, 1998.

Jakub, Jay and D. Phil. *Spies and Saboteurs: Anglo-American Collaboration and Rivalry in Human Intelligence Collection and Special Operations 1940-1945*. Palgrave, Basingstoke, UK, 1999.

Jeffreys-Jones, Rhodri. *The CIA and American Democracy*. Yale University Press, New Haven, CT, 1998.

Knight, Amy. *Spies Without Cloaks, The KGB's Successors*. Princeton University Press, Princeton, NJ, 1996.

Kornbluh, Peter, ed. *Bay of Pigs Declassified, The Secret CIA Report on the Invasion of Cuba*. The New Press, New York, NY, 1998.

Krivitsky, W.G., Sam Tanenhaus, and Santi Corvaja. *In Stalin's Secret Service: Memoirs of the First Soviet Master Spy to Defect*. Enigma Books, New York, NY, 2000.

Lamont-Brown, Raymond. *Kampeitai: Japan's Dreaded Military Police*. Sutton Publishing, Phoenix Mill, UK, 1998.

Leonard, Raymond W. *Secret Soldiers of the Revolution: Soviet Military Intelligence, 1918-1933*. Greenwood Publishing, Westport, CT, 2000.

Lindgren, David T. *Trust but Verify: Imagery Analysis in the Cold War*. Naval Institute Press, Annapolis, MD, 2000.

Lunev, Stanislav and Ira Winkler. *Through the Eyes of the Enemy: Russia's Highest Ranking Military Defector Reveals Why Russia Is More Dangerous Than Ever*. Regnery Publishing, Washington, DC, 1998.

Macdonald, Bill J. *The True 'Intrepid': Sir William Stephenson and the Unknown Agents*. Timberholme Books, Surry, British Columbia, Canada, 1998.

Maffeo, Steven E. *Most Secret and Confidential: Intelligence in the Age of Nelson*. Naval Institute Press, Annapolis, MD, 2000.

Mahl, Thomas E. *Desperate Deception: British Covert Operations in the United States, 1939-44*. Brassey's, New York, NY, 1998.

Marks, Leo. *Between Silk and Cyanide, A Codemaker's War 1941-1945*. Free Press, New York, NY, 1998.

Masetti, Jorge. *In the Pirate's Den: My Life as a Secret Agent for Castro*. Encounter Books, San Francisco, CA, 2001.

Melton, Buckner F. *Aaron Burr: Conspiracy to Treason*. John Wiley & Sons, New York, NY, 2001.

Mitrovich, Gregory. *Undermining the Kremlin: America's Strategy to Subvert the Soviet Bloc 1947-1956*. Cornell University Press, Ithaca, NY, 2000.

Morgan, Ted. *A Covert Life: Jay Lovestone, Communist Anticommunist and Spymaster*. Random House, New York, NY, 1999.

Osborn, Shane and Malcolm McConnell. *Born to Fly: The Untold Story of the Downed American Reconnaissance Plane*, Broadway Books, New York, NY, 2001.

Perisco, Joseph E. *Roosevelt's Secret War: FDR and World War II Espionage*. Random House, New York, NY, 2001.

Polmar, Norman and Thomas B. Allen. *The Encyclopedia of Espionage*. Grammercy, New York, NY, 1998.

Richelson, Jeffrey T. *The Wizards of Langley: Inside the CIA's Directorate of Science and Technology*. Westview Press, Boulder, CO, 2001.

Rigden, Denis. *Kill the Fuhrer: Section X and Operation Foxley*. Sutton Publishing, Phoenix Mill, UK, 2000.

Romerstein, Herbert and Eric Breindel. *The Venona Secrets: Exposing Soviet Espionage and America's Traitors*. Regeney Publishing, Washington, DC, 2000.

Roberts, Sam. *The Brother: The Untold Story of Atomic Spy David Greenglass and How He Sent His Sister Ethel Rosenberg to the Electric Chair*. Random House, New York, NY, 2001.

Rudgers, David F. *Creating the Secret State: The Origins of the Central Intelligence Agency, 1943-1947*. University of Kansas Press, Lawrence, KS, 2000.

Russell, Frank Santi. *Information Gathering in Classical Greece*. University of Michigan Press, Ann Arbor, MI, 2000.

Saunders, Frances Stonor. *The Cultural Cold War: The CIA and the World of Arts and Letters*. The New Press, New York, NY, 1999.

Sawyer, Ralph D. *The Tao of Spycraft: Intelligence Theory and Practice in Traditional China*. Westview Press, Boulder, CO, 1998.

Schecter, Jerold L. and Leona P. Schecter. *Sacred Secrets: How Soviet Intelligence Operations Changed*. Brasseys, Inc, New York, NY, 2002.

Seabag-Nibtefiore Hugh. *Enigma: The Battle for the Code*. John Wiley & Son, New York, NY, 2001.

Seaman, Mark. *Secret Agent's Handbook: The WW II Spy Manual of Devices, Disguises, Gadgets and Concealed Weapons*. The Lyons Press, New York, NY, 2001.

Shannon, Elaine and Ann Blackman. *The Spy Next Door*. Little, Brown, Boston, MA, 2002.

Shaw, Mark. *Miscarriage of Justice: The Jonathan Pollard Story*. Paragon House, St. Paul, MN, 2001.

Sheldon, Rose Mary. *Tinker, Tailor, Caesar, Spy: Espionage in Ancient Rome*. Frank Cass, Ltd., London, UK, 2001.

Shultz, Eichard H. Jr. *The Secret War Against Hanoi: Kennedy and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam*. Harper Collins, New York, NY, 1999.

Singh, Simon. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. Doubleday, New York, NY, 1999.

Smith, Michael. *The Emperor's Codes, The Breaking of Japan's Secret Ciphers*. Arcade Publishing, New York, NY, 2000.

Spence, Jonathan D. *Treason by the Book*. Viking, New York, NY, 2001.

Srodes, James. *Allen Dulles Master of Spies*. Regnery Publishing, Washington, DC, 1999.

Stafford, David. *Secret Agent: the True Story of the Special Operations Executive*. Overlook Press, Woodstock, NY, 2001.

Roosevelt and Churchill, Men of Secrets. Overlook Press, Woodstock, NY, 2000.

Churchill and Secret Service. Overlook Press, Woodstock, NY, 1997.

Steele, Robert David. *On Intelligence: Spies and Secrecy in an Open World*. AFCEA International Press, Fairfax, VA, 2000.

Stephenson, William Samuel (editor) *British Security Coordination: The Secret History of British Intelligence in the Americas 1940-1945*, Fromm International Publishing Group, 1999.

Steury, Donald Paul and Roger Cirillo, eds. *The Intelligence War (World War II Chronicles)*. Metro Books, London, UK, 2000.

Stober, Dan and Ian Hoffman. *Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage*. Simon & Schuster, New York, NY, 2002.

Tart, Larry and Robert Keefe. *Attacks on American Surveillance Flights: The Price of Vigilance.* Ballantine Books, New York, NY, 2001.

Trento, Joseph J. *The Boys From Berlin: The Secret History of the CIA*. Roberts Rinehart Publishers, Niwot, CT, 1999.

The Secret History of the CIA, Prime Publishing. Highland Park, IL, 2001.

Tourison, Sedgwick. *Secret Army Secret War Washington's Tragic Spy Operation in North Vietnam*. Naval Institute Press, Annapolis, MD, 1995.

Vise, David A. *The Bureau and the Mole: The Unmasking of Robert Philip Hanssen, the Most Dangerous Double Agent in FBI History*. Atlantic Monthly Press, Atlanta, GA, 2002.

Von Rintelen, Franz. *The Dark Invader: Wartime Reminiscences of a German Naval Intelligence Officer*. Frank Cass & Co., London, UK, 1998.

Warner, Roger. *Back Fire: The CIA's Secret War in Laos and its Link to the War in Vietnam*. Simon and Schuster, New York, NY, 1995.

Wasserstein, Allen and Alexander Vassiliev. *The Haunted Wood*. Random House, New York, NY, 1999.

Wasserstein, Bernard. *Secret War in Shanghai*.

Houghton Mifflin Co, Boston, MA, 1999.

Weber, Ralph E., ed. *Spymasters: Ten CIA Officers in Their Own Words*, Tyndale House Publishers, Carol Stream, IL, 1998.

Wen Ho Lee. *My Country Versus Me*. Hyperion, New York, NY, 2001.

West, Nigel. *The Crown Jewels: The British Secrets at the Heart of the KGB Archives*. Yale University Press, New Haven, CT, 1999.

Whiting, Charles. *Hitler's Secret War: the Nazi Espionage Campaign Against the Allies*. Casemate Publishers, Haverton, PA, 2000.

Whymont, Robert. *Stalin's Spy: Richard Sorge and the Tokyo Espionage Ring*. St. Martin's Press, New York, NY, 1999.

Wires, Richard. *The Cicero Spy Affair: German Access to British Secrets in World War II*. Praeger Publishing Trade, Westport, CT, 1999.

Wise, David. *Cassidy's Run*. Random House, New York, NY, 2000.

CI Calendar of Events

7 January 1998
Clyde Lee Conrad, a former US Army Sergeant who was convicted of treason in 1990, dies in a German prison in January 1999, where he was serving a life sentence.

26 January 1998
Steven L. David pleads guilty to federal charges that he stole and disclosed Gillette Company trade secrets. He was sentenced on 17 April 1998 to 27 months in prison.

11 February 1998
President Clinton issues Presidential Decision Directive-61 (PDD-61), which orders DOE to establish a stronger counterintelligence program.

26 February 1998
Arkady N. Shevchenko, a former high-ranking Soviet diplomat who defected to the United States on 6 April 1978, dies of a heart attack.

3 April 1998
FBI arrests CIA employee Douglas Frederick Groat on charges of espionage.

13 April 1998
New York Times reveals a May 1997 classified Pentagon report that concluded Hughes and Loral gave critical data to China that notably improved the reliability of its nuclear missiles.

11 May 1998
Israel officially acknowledges for the first time that Jonathan Pollard was an Israeli agent.

3 June 1998
James Clark, a one-time campus radical and former US Army paralegal, pleads guilty to conspiracy to commit espionage.

15 June 1998
The French magazine *Le Point* reports that France systematically listens in on the telephone

conversations and cable traffic of many businesses based in the United States and other nations.

17 June 1998
Department of Defense declassifies its first reconnaissance satellite, which was launched shortly after the 1 May 1960 shootdown of Francis Gary Power's U-2 over the Soviet Union.

25 July 1998
Russian President Boris Yeltsin appoints Vladimir Putin, a former KGB officer, to head the Federal Security Service from Nikolai Kovalev.

27 July 1998
CIA employee Douglas Frederick Groat pleads guilty to one count of attempted extortion after a plea agreement.

28 July 1998
FBI arrests Huang Dao Pei—a Chinese-born naturalized US citizen—on charges that, from 1992 to 1995, he tried to steal trade secrets of a hepatitis C monitoring kit from Roche Diagnostics and sell them to China.

1 August 1998
Joel Barr—an American communist and friend of Julius and Ethel Rosenberg—who barely eluded the FBI before he could be arrested for espionage in 1950, dies of complications of diabetes in a hospital in Moscow.

12 September 1998
Three-year FBI and other US Government agencies' investigation culminates in the arrest of a Cuban illegals network in Miami, Florida.

25 September 1998
Former CIA officer Douglas Groat gets five years in prison after pleading guilty to one count of extortion in return for prosecutors dropping four espionage counts.

5 October 1998
DOE Secretary Bill Richardson selects Lawrence H. Sanchez to be Director of the Office of Intelligence.

13 October 1998
FBI arrests retired US Army intelligence analyst David Sheldon Boone, charging him with selling secrets to Moscow.

6 November 1988
Kelly Warren, a former US Army soldier who served in Germany from 1984 to 1988, pleads guilty to one count of conspiracy to commit espionage.

13 November 1998
DOE Secretary Bill Richardson submits CI Action Plan to National Security Council.

5 December 1998
James M. Clark is sentenced to 12 years and seven months in prison for spying for East Germany and other countries.

20 December 1998
David Boone pleads guilty to conspiracy to commit espionage and is sentenced on 26 February 1999 to 24 years and four months in prison.

4 January 1999
Cox Committee submits its classified report to the President, which includes 38 recommendations addressing issues related to export control and counterintelligence.

22 January 1999
Theresa Marie Squillacote and her husband, Kurt Alan Stand, are sentenced to 21 and 17 years in prison on spy charges, respectively.

South Korea changes name of its spy agency to National Intelligence Service, apparently to dispel the agency's former tarnished image as a political tool of repression.

5 February 1999
British Government names Richard Dearlove as new Secret Intelligence Service (MI-6) chief, effective 1 September 1999.

12 February 1999
Kelly Warren is sentenced to 25 years in prison

on charges that she spied for Hungary and Czechoslovakia. She was part of the Clyde Lee Conrad espionage ring in Europe.

4 March 1999
DOE CI Implementation Plan (per PDD-61) is issued to Laboratories.

8 March 1999
DOE fires Wen Ho Lee, a computer scientist at Los Alamos, for allegedly leaking sensitive nuclear information to China.

9 March 1999
Based on faulty CIA information, NATO forces mistakenly bomb the Chinese Embassy in Belgrade.

18 March 1999
President Clinton requests the President's Foreign Intelligence Advisory Board (PFIAB) to review security threat at DOE's nuclear weapons laboratories and measures taken to address that threat.

31 March 1999
Kai-Lo Hsu, technical director of Yuen Foong Paper Co., Ltd., in Taiwan, pleads guilty to conspiring to steal Taxol formula from Bristol-Myers Squibb.

26 April 1999
Pin Yin Yang and Hwei Chen "Sally" Yang are convicted under Economic Espionage Act of 1996 of stealing corporate secrets from Avery Dennison.

17 May 1999
Former Australian intelligence official Jean Wispleare is charged with attempted espionage for selling secrets to an undercover FBI agent posing as a foreign spy.

15 June 1999
PFIAB presents the "Rudman Report" to President Clinton, which states DOE is a dysfunctional bureaucracy incapable of reforming itself.

July 1999
Russia expels US diplomat amid hints the case involved spying.

1 July 1999
Viktor M. Chebrikov, former KGB chairman (1982-88), dies unexpectedly at age 76.

13 July 1999
New Zealand Prime Minister appoints senior diplomat Richard Woods to head Security Intelligence Service, effective 1 November 1999.

22 July 1999
China outlaws Falun Gong, a spiritual sect in China whose leader, Li Hongzhi, has lived in New York since he left China in 1998.

4 October 1999
US Supreme Court rejects appeal by Robert Kim, who is serving a nine-year sentence for spying for South Korea.

1 November 1999
Theodore Alvin Hall, who passed Atom bomb secrets to Soviets, dies of cancer in Cambridge, England.

5 November 1999
US Navy First Class Petty Officer Daniel M. King is arrested after failing a routine polygraph examination.

18 November 1999
Russia's FSB domestic security service charges nuclear scientists Igor Sutyagin at Moscow's prestigious USA and Canada Institute with high treason.

29 November 1999
US military charges US Navy code breaker Daniel King with selling data to Moscow.

30 November 1999
Russian security officials advise catching Cheri Leberknight, a second secretary in the political section of the US Embassy, in the act of spying.

3 December 1999
President Clinton signs legislation, which creates an independent Agency for Nuclear Stewardship within DOE with authority for DOE's national security programs and nuclear weapons laboratories and production facilities.

8 December 1999
United States expels Stanislav Gusev, a Russian diplomat accused of monitoring a listening device planted in a State Department conference room.

10 December 1999
Wen Ho Lee, former DOE physicist, is indicted on 59 felony counts of mishandling national security information.

16 December 1999
United States and China reach agreement on compensation for damages arising out of accidental NATO bombing of the Chinese Embassy in Belgrade.

5 January 2000
P. Y. Yang of Taiwan-based Four Pillars, Ltd., is sentenced to two-years probation and six-months home detention for violating the 1996 Economic Espionage Act.

20 January 2000
Laptop containing thousands of pages of classified information disappears from State Department.

17 February 2000
Immigration and Naturalization Service employee Mariano Faget is arrested for espionage.

8 March 2000
Clinton Administration releases Unclassified version of an annual report on Chinese espionage in the United States.

8 March 2000
DCI, the FBI Director, and the Deputy Secretary of Defense unveil Counterintelligence *for the 21st Century* during a SSCI closed hearing. CI 21 restates and expands upon other recent assessments of the emerging CI environment.

17 March 2000
Armed Forces Court of Appeals suspends grand jury hearings in the case of accused spy Daniel King.

5 April 2000
Russian Federal Security Bureau detains retired US Navy intelligence officer, Edmond Pope, and a Russian accomplice for suspected espionage.

8 April 2000
US files espionage charges against Timothy Steven Smith, a civilian Defense Department employee assigned as an ordinary seaman aboard the USNS Kilauea, an ammunition ship.

14 June 2000
George Trofimoff, a retired Army colonel, is arrested and accused of spying for the Soviet Union in a 25-year-long Cold War conspiracy.

28 June 2000
Gen. John A. Gordon begins tenure as DOE Administrator of the National Nuclear Security Administration.

5 July 2000
European Parliament votes to investigate allegations that US using its surveillance apparatus, known as Echelon, to win commercial advantage for US companies.

7 July 2000
Ruth Werner, a communist spy who smuggled atom bomb secrets from Britain to the Soviet Union in the 1940s, dies at age 93.

9 August 2000
State Department offers $25,000 for return of missing laptop containing classified information.

13 August 2000
Federal appeals court upheld espionage conviction of Theresa Marie Squillicote and Kurt Alan Stand.

8 September 2000
Shigehiro Hagisaki, Japan Maritime Defense Force, is arrested after passing a classified document to

Russian GRU official Capt. Viktor Bogatenkov.

13 September 2000
Wen Ho Lee pleads guilty to one count of mishandling classified information and sentenced to time served.

27 September 2000
Russian prosecutors charge Edmund Pope with espionage.

28 September 2000
State Department announces suspension of security clearances for five employees for security violations.

13 October 2000
Gus Hall, longtime Communist Party leader in the United States, dies.

16 October 2000
NSA Director Lt. Gen. Michael V. Hayden announces major reorganization to let senior managers focus on reengineering SIGINT to handle major advances in communications technologies.

23 October 2000
Romania's Supreme Court annuls former diplomat Mircea Raceanu's death sentence, acquitting him of charges of passing state secrets to the United States during the Communist era.

4 November 2000
President Clinton vetoes 2001 Intelligence Authorization Act, which has provision allowing easier prosecution of US officials leaking classified information.

14 November 2000
National Commission for the Review of the NRO recommends creation of an Office of Space Reconnaissance to pursue innovative technology for spying from space.

27 November 2000
Shigehiro Hagisaki pleads guilty to passing defense secrets, including information on US Navy units in Japan to Russian military attache.

6 December 2000
Edmond Pope, sentenced to 20 years in prison, becomes first American convicted of espionage in Russia since U-2 pilot Francis Gary Powers in 1960.

15 December 2000
Russian President Vladimir Putin pardons Edmond Pope, who returns to the United States.

17 December 2000
Press reports President Clinton faces new round of lobbying for release of Jonathan Pollard, who spied for Israel; however, Clinton leaves office without granting the pardon.

26 December 2000
Russia admits that the KGB murdered Swedish diplomat Raoul Wallenberg, who saved thousands of Jews in Nazi occupied Hungary during WWII.

4 January 2001
President Clinton signs Presidential Decision Directive (PDD)-75 creating National Counterintelligence Executive, replacing NACIC.

12 January 2001
Vladimir Semichastny, KGB chief from 1961 to 1967, dies in Moscow at age 78.

18 January 2001
FBI ends investigation of two missing hard drives at Los Alamos National Laboratories without finding any evidence of espionage.

20 January 2001
President Clinton pardons former US Navy intelligence analyst Samuel L. Morrison, the government official ever convicted to leaking classified information.

1 February 2001
Russian FSB arrests John Edward Tobin on drug charges but says he is part of the US intelligence establishment.

11 February 2001
Chinese authorities detain Gao Zhan—a Chinese

scholar working at American University—her husband, and 5-year-old son.

16 February 2001
Former DOE Secretary Bill Richardson temporarily suspends measures, including giving polygraphs to 10,000 employees, pending a high-level review.

20 February 2001
FBI agent Robert Philip Hanssen is arrested for espionage on behalf of the Soviet Union/Russia.

25 February 2001
US citizen and Hong Kong businessman Li Shaomin is arrested crossing the border into Shenzhen, China.

8 March 2001
Jean Wispleare pleads guilty to charge of attempted espionage.

9 March 2001
US military officials dismiss all charges against Daniel King—accused of passing secrets to Moscow in 1994—because a trial would have exposed more secrets.

16 March 2001
Former British GCHQ employee Geoffrey Prime is freed from prison after serving half his 38-year prison sentence for passing UK secrets to the KGB.

20 March 2001
Media reports that Chinese PLA Senior Colonel Xu Junping was missing since last December during a visit to the United States.

21 March 2001
United States orders 50 Russian diplomats expelled as suspected spies in response to the Robert Hanssen espionage case.

23 March 2001
Russia orders 50 US diplomats to leave the country in its first retaliatory move over the expulsion of 50 Russian diplomats from the United States in a Cold War–style spy row.

31 March 2001
US Navy EP-3 aircraft monitoring Chinese military maneuvers collides with Chinese fighter sent to intercept it and makes emergency landing on Hainan island.

4 April 2001
China formally arrests Chinese-born US academic Gao Zhan on charges of accepting money from a foreign intelligence agency and participating in espionage activities in China.

8 April 2001
China detains Wu Jianming, a US citizen of Chinese origin, for alleged espionage activities against China on behalf of Taiwan.

12 April 2001
China releases the 24 American crewmembers of the US Navy EP-3 plane, which landed at the Chinese military base on Hainan island.

4 May 2001
FBI arrests Chinese scientists Hai Lin and Kai Xu and Chinese-born naturalized US citizen Yong Qing Cheng for attempting to send Lucent Technologies intellectual property to a Chinese state-owned technology firm.

7 May 2001
The United States resumes spy flights off the coast of China.

9 May 2001
Justice Department charges Takashi Okamoto and Hiroaki Serizawa, two Japanese scientists, with stealing cells and genetic materials from Cleveland Clinic Foundation, a top research center in Cleveland, then passing them along to a research institute in Japan.

26 May 2001
China arrests Chinese-born American Wu Juanmin on spying charges.

8 June 2001
Five Cubans, arrested on 12 September 1998, are convicted in Miami of conspiring to spy on the United States for Fidel Castro's communist regime.

26 June 2001
US Army Officer George Trofimoff is convicted of espionage.

29 June 2001
Mario Faget, who was convicted of disclosing classified information to Cuba, is sentenced to five years in prison.

5 July 2001
President Bush nominates federal prosecutor Robert Mueller as new Director of the FBI.

6 July 2001
Robert Hanssen pleads guilty to spying for Russia, avoids death penalty, gets life in prison; family to keep his FBI pension and house.

11 July 2001
US District Court dismisses appeal by Robert Kim against his nine-year prison term for spying for South Korea.

14 July 2001
China convicts US citizen Li Shaomin of spying for Taiwan and orders him deported.

24 July 2001
China convicts US-based scholar Gao Zhan of spying for Taiwan and sentences her to 10 years in prison. China also convicts US permanent resident and businessman Qin Guangguang of spying for Taiwan.

26 July 2001
China expels Gao Zhan and Qin Guangguang in effort to soothe relations with the United States.

24 August 2001
FBI arrests Brian Regan, a retired Air Force sergeant who worked for a government contractor and assigned to the National Reconnaissance Office, for espionage.

30 August 2001
US Customs arrests David Tzu Wvi Yang and Eugene You Tsai Hsu for attempting to export military encryption technology to China in violation of the Arms Control Act.

4 September 2001
FBI arrests Cuban "La Red Avispa" spy ring members George and Marisol Gari and charges them with espionage.

Former Justice Department prosecutor Robert Mueller becomes the sixth Director of the FBI.

20 September 2001
George and Marisol Gari pleads guilty to spy charges.

21 September 2001
FBI arrests Ana B. Montes, a senior analyst with the Defense Intelligence Agency, and charges her with espionage on behalf of Cuban intelligence.

27 September 2001
District Court judge sentences ex-Army Colonel George Trofimoff to life in prison for espionage on behalf of the Soviets.

28 September 2001
China frees Wu Jianmin after he "confessed to his crimes" and places him on an airplane to the United States.