SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the
U.S. Department of Energy

A Special Investigative Panel

President's Foreign Intelligence Advisory Board

JUNE 1999

ABSTRACT

On March 18, 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 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."

In response, the Honorable Warren B. Rudman, Chairman of PFIAB, appointed board members Ms. Ann Z. Caracristi, Dr. Sidney Drell, and Mr. Stephen Friedman to form the Special Investigative Panel and obtained detailees from several federal agencies (CIA, DOD, FBI) to augment the work of the PFIAB staff. Over the past three months, the panel and staff interviewed more than 100 witnesses, reviewed more than 700 documents encompassing thousands of pages, and conducted onsite research and interviews at five of the Department of Energy's national laboratories and plants: Livermore, Los Alamos, Oak Ridge, Pantex, and Sandia.

The panel has produced a report and an appendix of supporting documents, both of which are unclassified to the fullest extent possible. 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 the Department;
- The growth and evolution of the foreign intelligence threat to the national labs, particularly in connection with the Foreign Visitor's Program of the labs;
- The implementation and effectiveness of Presidential Decision Directive No. 61, the reforms instituted by Secretary of Energy Bill Richardson, and other related initiatives; and,
- Additional measures that should be taken to improve security and counterintelligence at the labs.

PANEL MEMBERS

The Honorable Warren B. Rudman, Chairman of the President's Foreign Intelligence Advisory Board. Senator Rudman is a partner in the law firm of Paul, Weiss, Rifkind, Wharton, and Garrison. From 1980 to 1992, he served in the U.S. Senate, where he was a member of the Select Committee on Intelligence. Previously, he was Attorney General of New Hampshire.

Ms. Ann Z. Caracristi, board member. Ms. Caracristi, of Washington, DC, is a former Deputy Director of the National Security Agency, where she served in a variety of senior management positions over a 40–year career. She is currently a member of the DCI/Secretary of Defense Joint Security Commission and recently chaired a DCI Task Force on intelligence training. She was a member of the Aspin/Brown Commission on the Roles and Capabilities of the Intelligence Community.

Dr. Sidney D. Drell, board member. Dr. Drell, of Stanford, California is an Emeritus Professor of Theoretical Physics and a Senior Fellow at the Hoover Institution. He has served as a scientific consultant and advisor to several congressional committees, The White House, DOE, DOD, and the CIA. He is a member of the National Academy of Sciences and a past President of the American Physical Society.

Mr. Stephen Friedman, board member. Mr. Friedman is Chairman of the Board of Trustees of Columbia University and a former Chairman of Goldman, Sachs, & Co. He was a member of the Aspin/Brown Commission on the Roles and Capabilities of the Intelligence Community and the Jeremiah Panel on the National Reconnaissance Office.

PFIAB STAFF

Randy W. Deitering, *Executive Director*

Frank W. Fountain, *Assistant Director and Counsel*

Mark F. Moynihan, *Assistant Director*

Brendan G. Melley, *Assistant Director*

Roosevelt A. Roy, *Administrative Officer*

Jane E. Baker, *Research/Administrative Officer*

PFIAB ADJUNCT STAFF

Roy B., *Defense Intelligence Agency*

Christine V., *Central Intelligence Agency*

Karen DeSpiegelaere, *Federal Bureau of Investigation*

David W. Swindle, *Department of Defense, Naval Criminal Investigative Service*

Jerry L., *Central Intelligence Agency*

Joseph S. O'Keefe, *Department of Defense, Office of the Secretary of Defense*

TABLE OF CONTENTS

continued

FOREWORD FROM THE SPECIAL INVESTIGATIVE PANEL

For the past two decades, the Department of Energy 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, they undoubtedly will 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 the Department 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.

At the birth of DOE, the brilliant scientific breakthroughs of the nuclear weapons laboratories came with a troubling record of security administration. Twenty years later, virtually every one of its original problems persists.

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 on library shelves accessible to the public at the Los Alamos laboratory. 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. Fiscal management was bedeviled by sloppy accounting. 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 naiveté.

Twenty years later, every one of these problems still existed. Most still exist today.

In response to these problems, the Department 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 shake–up 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* that the Department make fundamental changes in security procedures, compliance by Department bureaucrats was grudging and belated.

The panel found a department saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial.

Time after time over the past few decades, officials at DOE headquarters and the weapons labs themselves 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, the Department 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 own security experts. It has repeatedly attempted reforms. Yet the Department'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 in 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 to 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 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 vacates the 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 next Secretary of Energy will not have spent months at the tip of the sword created by the recent public outcry over DOE mismanagement of national secrets. Indeed, the core of the Department's bureaucracy is quite capable of undoing 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.

THE PFIAB INQUIRY

The PFIAB panel is fully aware of the many recent allegations of management failures surrounding the Department of Energy and questions about the subsequent roles of entities such as the Department of Justice, the Federal Bureau of Investigation, and the Central Intelligence Agency. Much of the research we conducted has relevance to these allegations. However, the depth and the complexity of the issues call for examinations by institutions with greater resources and a wider charter: namely, Congress and standing executive agencies of the federal government.

In the 90 days of our inquiry, the PFIAB panel conducted numerous interviews with senior federal officials who agreed to speak candidly—with the understanding that they would not be identified by name—about DOE's problems and recent events. On balance, the panel finds that some very damaging security compromises may have occurred, as alleged by some in recent weeks. But we believe that in matters of intelligence and counterintelligence, one cannot brush off the reality that conclusions are often intrinsically based on probabilities, rather than certainties.

Leaders, of course, are often obliged to act, and should act, based on the probability of impending danger, not only its certainty. And those entrusted with the public weal are indisputably served better by having more information about risks than less. So the panel would like to note the contributions of those who have helped to raise the public's awareness of the risks to national security posed by problems at DOE. Although we do not concur with all of their conclusions, we believe that both intelligence officials at the Department of Energy and the members of the Cox Committee made substantial and constructive contributions to understanding and resolving security problems at DOE. As we note later in this report, we concur on balance with the damage assessment of espionage losses conducted by the Director of Central Intelligence. We also concur with the findings of the independent review of that assessment by Admiral David Jeremiah and his panel.

Our mandate from President Clinton was restricted to an analysis of the structural and management problems in the Department's security and counterintelligence operations. We abided by that. We also recognize the unique nature of the assignment given to us by the President. Never before in its history of more than 35 years has the PFIAB prepared a report for release to the general public. As a result, we have taken pains to ensure that the language of this report is "plain English," not bureaucratese, and that the findings of the report are stated directly and candidly, not with the indirection and euphemisms often employed by policy insiders.

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 promote the building of a responsible culture over time. 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 semi–autonomous 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. The other alternative is a wholly independent agency, such as the National Aeronautics and Space Administration (NASA). There was substantial debate among the members of the panel about these two alternatives. Both have strengths and weaknesses. In the final analysis, the decision 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 nonclassified scientific research with the other DOE labs and the wider scien-

tific 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 cross–cutting 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.

The nuclear weapons and research functions of DOE need more autonomy, a clearer mission, a streamlined bureaucracy, and increased accountability.

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.

Warren Rudman
Chairman of the President's Foreign Intelligence Advisory Board

Ms. Ann Caracristi
Board Member

Dr. Sidney Drell
Board Member

Mr. Stephen Friedman
Board Member

FINDINGS

On March 18, 1999, President Clinton tasked the Foreign Intelligence Advisory Board to review the history of the security and counterintelligence threats to the nation's weapons labs and the effectiveness of the responses by the U.S. government. He also asked the Board to propose further improvements.

This report, based on reviews of hundreds of source documents and studies, analysis of intelligence reports, and scores of interviews with senior level officials from several administrations, was prepared over the past 90 days in fulfillment of the President's request.

BOTTOM LINE

Our 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.

The national labs of the Department of Energy are among 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—it has provided the nation with far–reaching advantages. Its discoveries not only helped the United States to prevail in the Cold War, they will 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 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 outlooks 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. So research done by U.S. 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 the secrets necessary to join the nuclear club.

Snapshot: DOE Weapons Operations

Percentage of Budget: Roughly $6 billion, a third of the Department's $18 billion FY99 budget.

Allocation of Weapons-Related Budget:

Defense Programs	$4.4 billion
Nonproliferation/Nat. Sec.	0.7
Fissile Material Disposal	0.2
Naval Reactors	0.7

Number of Contract Employees: 34,190

Number of Contract Employees Per Lab

Los Alamos	6,900
Sandia	7,500
L. Livermore	6,400
Pantex	2,860
Oak Ridge (Y-12)	5,500
Kansas City	3,150
Nevada Test Site	1,880

SOURCE: DEPT. OF ENERGY FIELD FACTBOOK, MAY 1998

More than 25 years worth of reports, studies and formal inquiries—by executive branch agencies, Congress, independent panels, and even DOE itself—have identified a multitude of chronic security and counterintelligence problems at all of the weapons labs (See Appendix). 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 cited for immediate attention and resolution … over and over and over … ad nauseam.

The open–source information alone on the weapons laboratories overwhelmingly supports a troubling conclusion: their security and counterintelligence operations have been seriously hobbled and relegated to low-priority status for decades. 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—both at DOE headquarters and the labs themselves—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, minimal budgets, and employed little more than crude "awareness" briefings of foreign threats and perfunctory and sporadic debriefings of scientists travelling to foreign countries.

- A lab security management reporting system that led everywhere but 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 real leadership and effective management at DOE.

The nature of the intelligence–gathering methods used by the People's Republic of China poses a special challenge to the U.S. 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 elicitations 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 U.S. security interests is, at the least, currently unknown; at worst, it may be unknowable. 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 also concur with the findings of the subsequent independent review, led by retired Admiral David Jeremiah, of that damage assessment.

The Department of Energy 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, the reform–minded management transitions out, either due to a change in administrations or as a result of the traditional "revolving door" management practices at DOE. 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 Watkins. The report skewered DOE for unacceptable "direction, coordination, conduct, and oversight" of safeguards and security. Two years later, the new administration rolled in, redefined priorities, and the initiatives all but evaporated. Deputy Secretary Charles Curtis in late 1996 investigated clear indications of serious security and CI problems and drew up a list of initiatives in response. Those initiatives also were dropped after he left office.

Reorganization is clearly warranted to resolve the many specific problems with security and counterintelligence in the weapons laboratories, but 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 to 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 national security and intelligence issues as well. The list of former Secretaries, Deputy Secretaries, and Under Secretaries meeting all of these criteria is very short. Despite having a large proportion of its budget (roughly 30 percent) devoted to functions related to nuclear weapons, the Department of Energy 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 decisionmaking 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 nonweapons research functions will require both disinterested scientific expertise, judicious decisionmaking, 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 U.S. weapons labs have achieved remarkable scientific advances and 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 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 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. Never have the members of the Special Investigative Panel 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 U.S. government resides at the national weapons labs, and this asset should be better used by the intelligence community. 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

AN INTERNATIONAL ENTERPRISE

U.S. research laboratories have always had a tradition of drawing on immigrant talent. Perhaps the first foreign–born contributor to our nation's nuclear program was Albert Einstein. In his letter to President Roosevelt on August 2, 1939, Einstein advised the President of the possibility of the atomic bomb and the urgent need for government action.

By 1943, the ranks of the Manhattan project at Los Alamos, New Mexico were filled with scientists and engineers from Italy (Fermi), Germany (Bethe), Poland (Ulam), Hungary (Wigner, Szilard, Von Neumann, and Teller), Russia (Kistiakovsy) and Austria (Rabi). Indeed, it is possible that the atomic bomb would never have been completed but for immigrant talent, and the diversity of talent applied to the project was hailed at the time as a model of international cooperation. Eleanor Roosevelt, in a 1945 radio address, declared that the development of the atomic bomb by "many minds belonging to different races and different religions sets the pattern for the way in which in the future we may be able to work out our difficulties."[2]

The role of and reliance on immigrant talent in the United States—particularly at the graduate school and doctoral levels where much of the nation's research is performed—has increased over the years. From 1975 to 1992, the aging of America's baby boomers resulted in a decline in the overall size of the college–age population and, unlike other industrialized nations, the U.S. saw a decline in the number of American students receiving science and engineering degrees.[3]

From the 1950s until 1995, the number of non–U.S. citizens who earned doctorates in scientific and engineering fields from American universities steadily climbed, reaching 27 per-

cent by 1985 and 40 percent by 1995. Two–thirds of those receiving those doctorates in 1995 held temporary residency visas, and Chinese doctoral recipients outnumbered recipients from all other regions combined.[4]

But the willingness to draw on foreign talent also has meant a greater risk of falling prey to those with foreign allegiances. One of the earliest and most infamous espionage scandals at the nation's nuclear laboratories was centered on the physicist Klaus Fuchs, a German native and naturalized British citizen who spied on researchers at Los Alamos for the Soviet Union. More recent instances of actual and alleged foreign espionage at the nuclear weapons laboratories are detailed in the Classified Appendix to this report.

As growth of the U.S. talent pool in science and engineering stagnated, and the amount of available talent abroad grew rapidly, the U.S. has had to rely on more foreign–born talent in national scientific research and development programs in order to maintain the best research facilities in the world. At the same time, since the end of the Cold War, DOE has entered into more extensive cooperative programs with foreign nations in efforts to reduce the threats of proliferation and diversion of nuclear weapons material. By June 1990, DOE had entered into 157 bilateral research and development agreements for scientific exchange purposes. Among others, parties to the agreements were the Soviet Union, the People's Republic of China, Soviet bloc nations and countries that posed nuclear proliferation threats.[5] In December 1990, a report to the DOE Secretary noted "a high probability of greatly increasing numbers of foreign visits and assignments to DOE facilities in future years."[6] The widening of foreign contacts concurrent with a greater influx of foreign–born talent has raised concerns about security compromises by scientists with foreign allegiances and highlighted the need for special care in implementing formal clearance procedures for involvement in classified work.

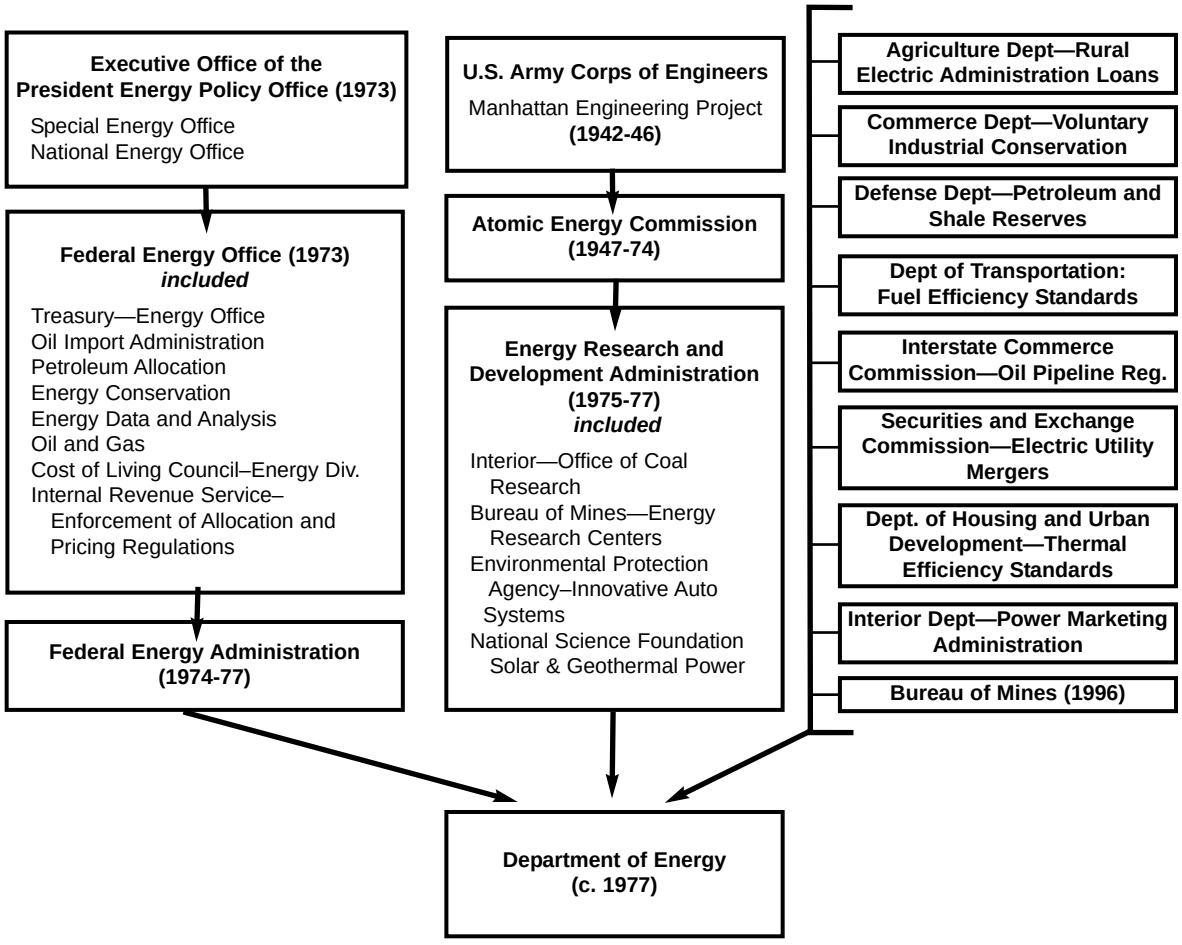
BIG, BYZANTINE, AND BEWILDERING BUREAUCRACY

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 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 U.S. 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.

Birth by Fusion: The Department of Energy



***Fusion or Confusion?*: The first annual report of the newly created Department of Energy declared that combining "the energy–related functions hitherto invested in many federal agencies [would provide] a new and sharpened sense of coherence, direction, and focus to the U.S. Government's role in meeting the challenge of creating a new and more secure energy base for the future." Tellingly, discussion of the security of the nation's nuclear weapons information and materials occupied less than 2 percent of the report's contents.**

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

The DOE Management Challenge

MISSION

- Lead agency for development of national energy resources and technologies.
- Responsible for the largest environmental cleanup effort in history.
- Nuclear energy and weapons research and development.
- Management of special nuclear materials stockpiles.
- Protection of highly sensitive classified and proprietary information against foreign and corporate espionage.

SIZE

- If included among the Nation's Fortune 500 firms, would rank in the top 50.
- The fourth largest landowner in the United States.
- Budget of roughly $18 billion comprises close to 3 percent of total discretionary spending at the federal level.
- Employs more than 11,000 Federal employees and more than 100,000 contract employees.
- Owns and manages more than 50 major installations spread across 2.4 million acres and 35 states.

COMPLEXITY

- A diverse workforce of military and civilian personnel; U.S. citizens and foreign nationals; career federal officials and part-time researchers; white collar bureaucrats as well as scientists and engineers specializing in narrow esoteric fields.
- Constituencies include the White House, Congress, the power industry, multinational defense and aerospace corporations, major universities, states and municipalities seeking or monitoring environmental cleanups.

During 1978, its first year of operation within the new structure, DOE already had in place more than 9,500 prime contracts and more than 1,800 financial assistance awards, which together were spread among 188 universities and more than 3,200 contractors. And the Department was growing: from 1977 to 1978, grants and contracts with university researchers posted an increase of 22 percent.[7]

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 different 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."[8]

The problem is not only the diffuse nature of authority and accountability in the Department. It is 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 of these dynamic variables contribute to volatility in the Department's workforce 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 dozen years, DOE has averaged some kind of major departmental shake–up every two to three years. During that time, security and counterintelligence responsibilities have been "punted" from one office to the next.

CULTURE AND ATTITUDES

In the course of this inquiry, many officials interviewed by the PFIAB panel cited the scientific culture of the weapons laboratories as a factor that complicates, perhaps even undermines, the ability of the Department to consistently implement its security procedures. Although there seemed to be no universally accepted definition of the culture, nearly everyone agreed that it is distinct and pervasive.

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 only tend to 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 the Department of Energy 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.

Over 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

Over 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, DOE spending on safeguards and security decreased by roughly one–third.[1]

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 for 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 & 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, email, 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[2] 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.[3]

Improving physical security in a wide array of nuclear weapons facilities whose replacement value was an estimated $100 billion[4], 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,[5] 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."[6]

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 U.S. national security. DOE facilities and personnel remain priority targets for hostile intelligence collection."[7] Anecdotal evidence corroborates, and intelligence assessments agree, that foreign powers stepped up targeting of DOE during the early 1990s. (See 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.[8] 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 decisionmaking 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

How Long Does It Take?

Each year DOE security officials compile audits to identify security lapses and vulnerabilities in the facilities and procedures of the nuclear weapons laboratories and plants. The following year, they report on whether the problems have been addressed. Given the sensitivity of what was being protected—information about how to build, miniaturize, store, and maximize the destructiveness of nuclear weapons—the numbers logged in the audits are remarkable:

11 **No. of months a DOE employee was dead before Department officials realized four documents with CLASSIFIED and RESTRICTED DATA were still assigned to him.**

20 **No. of months before DOE officials could ensure that improperly stored classified computer media had been properly safeguarded.**

24 **No. of months it took to order security labels (SECRET, TOP SECRET, etc.) for mislabeled software.**

31 **No. of months that 2,750 out of 3,000 non-classified computer terminals were connected and being used on a classified network.**

31 **No. of months to write and approve a network security plan.**

35 **No. of months it took DOE officials to write a work order to replace a lock at a weapons lab facility containing sensitive nuclear information.**

45 **No. of months taken to correct a broken doorknob that was sticking in an open position and allowing access to sensitive areas.**

51 **No. of months to correct mistake that allowed secure telephone cryptographic materials to go improperly safeguarded.**

? **No. of months before security audit team discovered that the main telephone frame room door at a weapons lab had been forced open and the lock destroyed.**

SOURCE: DEPT. OF ENERGY

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.[9]

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.[10] A DOE annual 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."[11]

The counterintelligence effort at DOE in the late 1980s and mid–1990s was in its infancy and grossly underfunded. 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.

DOE requested an FBI agent detailee in 1988 to assist in developing a CI program, but the agent found that DOE failed to provide management support or access to senior DOE decisionmakers. 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 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."[12]

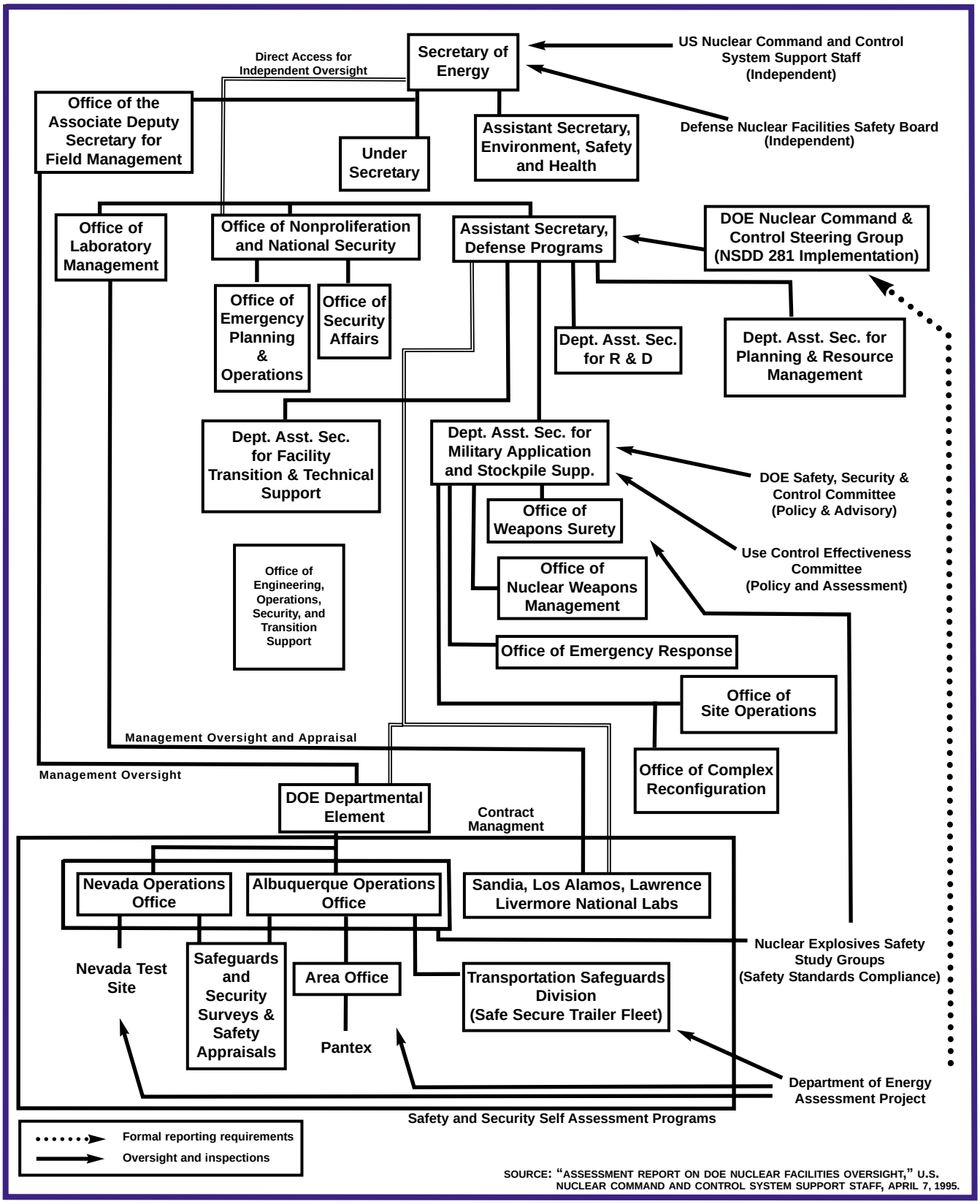
We asked a number of DOE officials to whom they report, to whom they were responsible. Invariably, their answer was: "It depends."

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.[13] 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

DOE Nuclear Programs Management/Oversight Structure Prior to 1999 Reforms



SOURCE: "ASSESSMENT REPORT ON DOE NUCLEAR FACILITIES OVERSIGHT," U.S. NUCLEAR COMMAND AND CONTROL SYSTEM SUPPORT STAFF, APRIL 7, 1995.

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.[14]

When DOE did devote its considerable resources to security, it too often faltered in implementation. A report 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."[15]

Foreign agents could probably not shoot their way into U.S. weapons laboratories. But they could apply for an access pass to walk in and strike up a conversation.

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.[16]

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 U.S. 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.[17]

Clearances to secure DOE areas have been granted simply for convenience, such as to reduce the length of an employee's walk from the car to the office each morning.

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."[18] 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.[19] 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 $18.6 million.[20]

- 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.[21]

- 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 semitrailer, some $21 million in inventory was written off.[22]

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."[23]

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.[24]

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.[25]

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.[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.[26]

But problems persisted. DOE Inspector General reports in 1990 and 1991 found that one of the weapons laboratories had granted "Q" clearances (which provide access to U.S. government nuclear weapons data) to more than 2,000 employees who did not need access to classified information.[28] 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."[29]

Three years later, a review of personnel security informed the Secretary 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."[30]

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.[31] 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.[32]

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 the 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.[33]

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."[34]

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."[35] 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."[36]

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."[37]

Some reports made extra efforts to puncture through the fog of bureaucratic language. A 1995 report to the President said: "By placing sensitive information on information systems, we increase the likelihood that inimicable 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."[38] In other instances, personnel were found to be sending classified information to outsiders via an unclassified email system.[39]

Even though the hard evidence points to only sporadic penetrations of the labs by foreign intelligence services (*see classified appendix*), 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."[41]

Ahead of its Time

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."[40]

The warning turned out to be on the mark. In April of this year, Energy Secretary Bill Richardson issued a 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 ... ."

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."[42]

TRACKING OF NUCLEAR MATERIALS: HOW MUCH MUF?

MUF stands for "materials unaccounted for," the official term used until the late 1970s for discrepancies in the amount of nuclear materials that can be physically located in inventory versus the amount noted in Department records. MUF (now termed with the more politic phrase "inventory differences") has been a recurring concern—and debate—in the nuclear research field since the beginning. The question at the center of the debate: if large quantities of nuclear material are impossible to measure with absolute precision, what constitutes a significant loss?

As in many questions, the answer depends on whom you ask. Officials of nuclear research facilities have argued that the scale and complexity of the processing and handling of nuclear material inevitably result in losses that are detectable but inconsequential. Outside observers have tended to be less sanguine about what constitutes a significant loss from a security standpoint.

In 1976, the General Accounting Office reported that the Nuclear Regulatory Commission and the Energy Research and Development Administration (DOE's predecessor) could not account for 8,000 pounds of highly enriched uranium and plutonium. Officials of the two agencies responded that part of the accounting discrepancy could be ascribed to the statistical margin of error in their measuring equipment, the rest was probably dregs created during processing and left in machinery parts, wiping cloths, and scrap items.[43]

Critics of the agencies have pointed out that thieves could easily use the variance in statistical measures to cover their tracks, stealing an increment during each measuring period that falls just within the margin of error. They have also pointed out that if Department records are not accurate, it is impossible for anyone to estimate the stock of nuclear material at any given point, much less the difference between two levels as it proceeds from one stage of the nuclear cycle to the next. In December 1994, the Department released updated figures for the cumulative amount of MUF or inventory difference for the 50-year period beginning in 1944. The cumulative figure: 6,174 pounds. Of that amount, a cumulative total of about 10 pounds was ascribed to "accidental losses" and "approved write-offs."[44]

GAO has continued to highlight the issue since DOE has become the steward of the nation's nuclear weapons laboratories. GAO published a report in 1991 criticizing the insufficiency of the Department's measuring systems and handling procedures[45]; in 1994, criticizing its methods of tracking exported nuclear material;[46] and in 1995, for installing a new system that was allegedly faulty.[47]

Even if accurate systems of measurement and accounting had been in place, it is not clear whether DOE officials would have been qualified to manage them effectively. A 1995 report to the President warned that "severe budget reductions, diminished technical resources, increased responsibilities, and reduced mission training ... have undermined protection of special nuclear material and restricted data."[48]

Last year, a report by an external review panel found "a lack of nuclear physical security expertise at all levels in the oversight process; ad hoc structuring of safeguards and security functions throughout the Department, and placement of oversight functions in positions which constrain their effectiveness."[49]

The dispute over the accuracy of nuclear measurements, of course, is beyond the technical capabilities of this panel to resolve. But the panel members do believe that its persistence and the low priority given to the issue relative to other DOE scientific goals is indicative of the institutional attitude that DOE has had toward security: nonscientists have a poor understanding of all things nuclear, so their judgments about acceptable levels of risk are suspect prima facie.

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.

But for more than a decade, the increasing prominence of foreign visitors in the weapons labs has increased concern about security risks. The PFIAB panel found that as early as 1985, the DCI raised concerns about the foreign visitors' program with the Energy Secretary. 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.[50]

The following year, 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 well behind 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."[51]

By September, 1992, DOE had instituted Visitor Assignment Management System (VAMS) databases, used 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 cross-checking of prospective visitors. Moreover, labs frequently did not even use the database and failed to enter visitor information. Instead, each lab developed its own computer program independently.

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 touch on classified information.

In 1994, DOE headquarters delegated greater authority to approve nonsensitive 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."[52]

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 only required for visitors from sensitive countries who visited secure areas or discussed sensitive subjects.

An internal DOE task force in 1996 determined that the Department's definitions of sensitive topics were not specific enough to be useful. It 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.[53] 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, U.S. 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.[54] The study found that records checks were still not being conducted regularly on foreign visitors from sensitive countries. [55]
Last year, 7,600 foreign scientists paid visits to the weapons labs.[56] 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.[57]

Administration Track Records

CARTER
(Schlesinger: Aug '77-Aug '79; Duncan: Aug '79-Jan '81)

'77 DOE established … First visiting U.S. scientists to China in '79 and '80 face Chinese elicitation effort. …**Late 1970s** FBI investigates possible espionage at a lab. …**'80** GAO reports on problems safeguarding against the spread of nuclear weapons technology.

REAGAN I
(Edwards: Jan '81-Nov '82; Hodel: Nov '82-Feb '85; Herrington: Feb '85-)

'82 DOE's Inspection and Evaluation program formed …GAO reports safeguards and security of weapons labs not adequate, recommends independent assessments program. …**'83** DOE issues threat guidance to provide a "consistent basis" for identifying vulnerabilities. …Memo to DOE, DOD states President has "decided to strengthen WH role … concerning the security of U.S. nuclear facilities."… President signs National Security Decision Directive (NSDD) on DOE security. … DOE Safeguards and Security Steering Group formed at President's direction to oversee fulfillment of physical security improvements … GAO reports security concerns at Rocky Flats facility. … DOE conducts eight internal security inspections at weapons facilities and DOE HQ; provides criticisms and recommendations to DOE management. … **'84** DOE's Central Training Academy established for protective force personnel.

REAGAN II
(Herrington: Feb '85-Jan '89)

'86 Rep. Dingell letter to President re: lab security vulnerabilities, management problems and lack of confidence in DOE. … Four GAO reports on DOE security and CI problems … External report requested by DOE finds problems with management of foreign visitors and adequate security. **…'87** Three GAO reports on DOE highlight the transfer of technology to proliferating nations and inefficient security clearance program. …Seven internal DOE security inspections criticize management and security practices in **'87-'88. …**DOE initiates the Personnel Security Assurance Program (PSAP) … DOE focuses on insider protection and strengthens classified document controls. …Three DOE IG reports about security clearance problems from **'86-'88. …'88** Intelligence Community paper reflects concerns with international scientific exchanges at the DOE labs. … President signs NSDD on Nuclear Weapons Safety, Security, and Control. … FBI detailee

to DOE cites inaccessibility to senior DOE managers. …President states "Improved nuclear security is an important legacy for us to leave the next administration;" DOE official opines that Energy has done "essentially all that can be done against the outsider threat." … Senate Intelligence Committee staff briefed on CI activities at labs. … Four GAO reports address DOE security and counterintelligence problems, including: major weaknesses in foreign visitor controls at labs, and foreign agents possibly gaining access to labs.

BUSH
(Watkins: Mar '89-Jan '93)

'89 New Secretary concerned about 1988 GAO criticism of DOE CI/security, defers DOE annual report on security until he reviews issue; NSC concurs. … GAO finds insufficient control over weapons-related information and technology. …**'90** Four IG reports on security … Secretary of Energy Advisory Board (SEAB) chartered … Interagency CI group prepares assessment of intelligence threat to government facilities from visiting foreign nationals. …GAO cites lack of clear, concise physical security standards and inconsistent material measurements at labs. … Freeze Task Force critical of split management of classified and unclassified computer security; finds direction, coordination, conduct and oversight of safeguards and security activities throughout DOE warrant structural changes. …External CI review highlights DOE's inability to manage comprehensive approach to foreign threat; inadequate oversight, control over secret document inventory; uncoordinated computer security responsibilities. …**'91** Four IG reports criticize security…GAO reports property, classified document control problems at LLNL; 10,000 documents unaccounted; inability of DOE to track, monitor, and correct security deficiencies … **'87, '89, and '91** GAO reports foreign countries routinely obtaining unclassified but sensitive information that could assist nuclear programs. …Memo to President highlights previous security problems at DOE, Secretary's efforts to fix the deficiencies. **…'92** Two IG reports on security…SSCI-requested CI assessment finds DOE headquarters lacks authority to direct labs, CI resources, and current threat information. …GAO cites weak internal security oversight controls; incomplete safeguards and security planning at DOE facilities. …DOE Order on CI issued. …DOE and FBI formalize relationship for conduct of CI activities. …Internal security report to Secretary finds "personnel are seldom held responsible for their disregard, either intentional or unintentional, of security requirements." … Another report finds "Problems in management and oversight represent the most significant weakness" for the Department…and "security systems continue to be plagued with potential single point failures."

ASSESSMENTS

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, obfuscations, 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; scores of DOE Office Directors and Lab managers; and a multitude of 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 incompetency 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 panel 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. Nor was it 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. We offer an analysis of some of these initiatives, and their likelihood of success, elsewhere in this chapter and elsewhere in this report.

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 (see box on previous administrations, on pp. 26-27), 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 figleaf.

The fact is that 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 that the Bush Administration took over; and higher still 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 U.S. intelligence agency obtained information that has come to be called the "walk-in" document. A copy of a classified PRC report, it contains a discussion of various U.S. 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 U.S. 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

U.S. thermonuclear warheads. This information had been widely available within the U.S. 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 U.S. 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 on 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 DOJ and FBI. In fact, as we understand it, that is the purpose of a task force recently appointed by the Attorney General. We trust that among the issues that the task force will resolve are:

- Whether the FBI committed sufficient resources, including agents with appropriate expertise, and demonstrated a sense of urgency commensurate with an apparent compromise of classified U.S. nuclear weapons information;

- Whether the DOJ Office of Intelligence Policy Review (OIPR) applied an inappropriately high standard to the FBI's request for electronic surveillance under the Foreign Intelligence Surveillance Act (FISA);

- Whether the FBI provided to DOJ OIPR all U.S. government information relevant to an appropriate evaluation of the FBI's FISA request;

- Why the FBI's FISA request did not include a request to monitor or search the

Clinton Administration Track Record

O'Leary: Jan '93–Jan '97

'93 New Secretary works to make labs more open…launches major declassification effort. … **DOE '92** Annual Report to President does not mention security problems highlighted same year in reports to Secretary …. GAO criticizes DOE's ineffective management of personnel security cases. …Four IG reports on security…Internal report to Secretary on computer security uncovers lack of access controls; no configuration management; failure to perform management reviews. …**'94** Three IG reports on security…FBI detailees to DOE recalled because of "lack of control of the CI program by DOE HQ." …Internal report finds classified and unclassified information on lab computer network. …GAO reports computer security deficiencies found in 1985 at six facilities still not fixed. …**'95** Four IG reports on security…Congress considers numerous bills between '95–'99 to abolish DOE. … "Galvin Task Force" offers SEAB options for change within the labs. … "Walk-in" provides documents containing sensitive U.S. nuclear information. …DOE officials meet with FBI regarding potential espionage involving nuclear weapons data. …Analysis group formed at DOE to review Chinese weapons program; senior DOE, CIA, White House officials discuss options. … GAO reports on poor management of nuclear material tracking capabilities …Laboratory Operations (oversight) Board created. …**'96** First three lab-to-lab exchanges between U.S. and China. …Internal DOE report discovers required nuclear material physical inventories not being performed. … Two IG reports on security…DOE Deputy Secretary directs six "initiatives" to lab directors and field office heads for the foreign visitors and CI programs (most initiatives ignored after he leaves DOE in 1997.)

Pena: Mar '97–Jun '98

'97 Mar New Secretary confirmed. … FBI report to Congress and DOE critical of DOE CI capabilities; addresses CI program oversight, foreign visits and assignments, CI analysis, professional training/CI awareness. … FBI Director personally delivers CI review to Secretary. …Two additional Lab–to–Lab exchanges held in Beijing. … DOE staff briefs Congressional staff, and NSC, CIA, FBI senior officials on Chinese nuclear program, possible Chinese espionage before Secretary informed…DOE increases budget for CI in **FY 1997,** hires more CI professionals. …Inter-agency Working Group reports that systemic and serious CI and security problems at DOE have been well documented over at least a ten year period … few of the recommendations in the past studies have been implemented, … A senior CI official states "There is every reason to believe the labs will resist" any outside assistance … National Security Advisor requests independent assessment of China's nuclear program and the impact of U.S. nuclear information. …Two DOE internal reports cite confusing, fragmented, dysfunctional security management structure. …External report finds multiple, uncoordinated internal and external oversight activities. …DCI and FBI Director meet with Secretary to discuss DOE CI problem and reform plan; … meeting notes state "Despite all the studies conducted, experience over time has shown that DOE's structure and culture make reform difficult, if not

impossible, from within." … Internal DOE report states "in all candor, we have been hampered in meeting [the safeguards and security] obligations by organizational obstacles and competing internal interests." … PDD–61 drafted, coordinated in inter-agency process. …DOE's Laboratory Operations Board finds "inefficiencies due to the Department's complicated management structure." …Peter Lee (formerly of LLNL) pleads guilty, inter alia, to transmitting classified national defense information to representatives of the PRC in '85. …GAO finds faulty procedures for foreign visitor indices checks and controlling dissemination of sensitive information; lack of clear criteria for identifying visits that involve sensitive subjects; indirect and inconsistent CI funding; DOE CI programs not based on comprehensive assessment of foreign espionage threat. …Institute of Defense Analyses' "120 Day Report" finds inadequate management of DOE workforce and confusing chains of command. …**'98** Feb. President signs PDD-61. …External report says DOE management and oversight of security problematic …Security Management Board created by Congress, meets twice in next 18 months…CIA/FBI report provided to Congress on Chinese espionage activities. … Jun 30 Secretary resigns, Deputy designated as Acting Secretary. … DOE's 90-day report on CI reveals problems remain regarding separate management of classified and unclassified information. …Lab-to-lab exchange held in Beijing.

Richardson: Aug '98 –
'98 Aug 18 New Secretary sworn in …GAO again finds problems in DOE's foreign visitor program; notes lack of clear procedures for identifying sensitive subjects. …External report highlights lack of DOE oversight expertise and ad hoc security structure. … Per PDD–61, assessment of the foreign collection threat against DOE published. …**'99** DOE security review finds "unhealthy, adversarial environment of mistrust among DOE security organizations," recommends several management process changes …Cox Committee publishes report…Lab-to-Lab exchange held in Beijing. …President directs PFIAB to review security, CI at labs; directs Intelligence Community to conduct damage assessment of possible security breaches at labs; directs CI community to review security of nuclear weapons information in USG. …DOE CI Implementation Plan delivered to Secretary. …GAO reports inadequate separation of classified and unclassified computer networks at same lab in **1988, 1992, 1994, and 1998. …** "Chiles Report" describes management problems in nuclear weapons program. …Internal DOE report highlights computer security problems at a lab. … DOE counterintelligence implementation plan (per PDD–61) issued to labs. … DOE shuts down all classified computers at LANL, LLNL, and SNL. … DOE holds tri-lab computer security conference. … Secretary announces new security organization at DOE, to be headed by a "security czar."

subject's workplace computer systems, particularly since an attorney in the FBI's General Counsel Office had provided an opinion in 1996 that such monitoring or searching in this case would require FISA authorization;

- Why the FBI did not learn until recently that in 1995 the subject had executed a series of waivers authorizing monitoring of his workplace computer systems;

- Whether the FBI adequately raised to the Attorney General the FBI's concerns over the declination of the FISA request;

- Whether communications regarding the subject's job tenure broke down between DOE, FBI, and Los Alamos.

- Whether the DOJ OIPR maintained appropriate records concerning FISA requests that were declined;

- Whether the FBI appropriately relied on technical opinions provided by the DOE;

- Why DOE, rather than the FBI, conducted the first polygraph examination in this case when the case was an open FBI investigation; and, perhaps most importantly,

- Whether additional cases should be opened to investigate whether the apparent disclosures may have arisen out of organizations other than Los Alamos lab.

Again, resolving these issues is not within our mandate. 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. Those steps are discussed further in the Classified Appendix to this report.

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 70s have not necessarily been rigorously adapted to fight the counterintelligence bat-

tles of the 90s (and beyond). For example, with the passage of more than twenty 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 Department of Justice 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. This goal is often furthered by leaving an espionage suspect in place to facilitate the gathering of more evidence. 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 U.S. 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 U.S. nuclear weapons information and the resultant threat to U.S. 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. The full text of the assessment's unclassified summary appears in the unclassified appendix.

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.[1] In late July, 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 U.S. nuclear information, and he directed that the National Counterintelligence Policy Board (NACIPB)[2] review the DOE counterintelligence program. That September, 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 an October 15 meeting, the Director of Central Intelligence 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 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. 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."

That winter, the NSC coordinated a draft PDD between and 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 in–fighting, these issues were finally resolved, or so it seemed; and on February 11, 1998, the President signed and issued the directive as PDD-61.

The full PDD remains classified. An unclassified summary, which contains all significant provisions, is set forth in the unclassified annex. 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;

- The incoming Director, OCI would prepare a report for the Secretary of Energy ninety days after his arrival 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; and,

- 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 April 1, 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 it to the Secretary of Energy on July 1, the day after Secretary Pena resigned. The Acting Secretary led a review of the study and its recommendations. On August 18, Secretary Richardson was sworn in. On November 13, he submitted the action plan required by the PDD to the National Security Advisor. Secretary Richardson continued to develop an implementation plan. The completed implementation plan was delivered to Secretary Richardson on February 3, 1999, and issued to the labs on March 4.

TIMELINESS OF PDD–61

Criticism has been raised that the PDD took too long to be issued and has taken too long to implement. Although the current National Security Advisor was briefed on counterintelligence concerns by DOE officials in April of 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. That there were disagreements over various issues is not surprising; that the DOE bureaucracy dug in its heels so deeply in resisting clearly needed reform is very disturbing. 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. It is not unreasonable to expect that senior DOE officials would require some time to evaluate the new OCI

Director's 90–day study, and we are aware that Secretary Richardson did not assume his DOE duties until mid–August. However, 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, 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 officials to requests for funding to implement the counterintelligence reforms mandated by PDD-61. We find vexing the reports we heard of OMB budgeteers lecturing other government officials on the "unimportance" of counterintelligence at DOE.

SECRETARY RICHARDSON'S INITIATIVES

Since November of 1998 and especially since April of this year, Secretary Richardson has taken commendable steps to address DOE's security and counterintelligence deficiencies. In November of last year, 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 Office of Counterintelligence (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 of 1999, in an effort to eliminate multiple reporting channels and 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 of 1999, Secretary Richardson announced substantial restructuring of the security apparatus at DOE. Among these is the new Office of Security and Emergency Operations, responsible for all safeguards and security policy, cyber–security, and emergency functions throughout DOE. It will report directly to the Secretary and consist of the Office of the Chief Information Officer, and Office of Emergency Management and Response, and an 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.

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. New controls will also 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. Cyber–security 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 of 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 stand–down 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 U.S. 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 us:

- There is a heightened attention to security at the most senior levels of DOE and the labs, but at the mid–level 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. It had not been checked by guards since August 1998. When confronted with the violation, a mid–level 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 email for possible security lapses. The lab took the minimal action necessary; it began monitoring emails but did not monitor the files attached to emails.

- 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.

BACK TO THE FUTURE

In 1976, federal officials conducted a study of the nation's nuclear weapons laboratories and plants. In trying to devise a coherent and viable way of managing the labs, they settled on three possible solutions: place the weapons labs under the Department of Defense, make them a free–standing agency, or leave them within the Energy Research and Development Administration. Congress chose to leave the weapons labs within ERDA, the successor agency of the Atomic Energy Commission.

Nearly a decade later, the oversight of the weapons labs was still of great concern. Senators Sam Nunn and John Warner led a push to place the weapons labs under the auspices of the Department of Defense. However, the Reagan Administration staved off their effort by agreeing to put together a blue–ribbon panel to study the issue. The panel studied the problem for six months and issued a report in July, 1985. Again, Congress and federal officials weighed whether the weapons labs should be transferred to the Department of Defense or restructured to be given more autonomy.

The status quo prevailed. The weapons labs stayed within the Department of Energy.

As this report has detailed, problems in the managerial relationship between DOE and the weapons labs have persisted, perhaps even increased, over the past 14 years. Indeed, the discussion today sounds hauntingly familiar to the discussions in the 1980s and 1970s.

Today, however, there is a difference. The record of mismanagement of the weapons labs in matters of security and counterintelligence has become so long and so compelling as to demand a rejection of the status quo. There can be no doubt that the current structure of the Department of Energy has failed to give the nation's weapons laboratories the level of care and attention they warrant. Thus, our panel is recommending deep and lasting structural change that will give the weapons laboratories the accountability, clear lines of authority, and priority they deserve.

REORGANIZATION

What makes a government agency run well? There are a multitude of characteristics that arguably can make for an efficient and effective government agency or department. This Panel holds no illusions about the completeness of its understanding nor the purity of its wisdom regarding government bureaucracies. Indeed, some people would say that truly comprehending the inner workings of a federal department is the intellectual equivalent of grasping the enormity of the universe. Over the course of many years, however, we, as members of the President's Foreign Intelligence Advisory Board, have evaluated the performance of numerous federal entities, from the Department of Defense to the Foreign Broadcast Information Service. Some, we found, were in good order, others in pretty bad shape. In that sense, we believe we do know a lot about what makes some agencies work and not work. Although somewhat subjective and by no means exhaustive, our list of "good" things to look for includes several attributes.

LEADERSHIP

Certainly at the top, but also throughout the organization. The leaders and managers set the standards and expectations regarding performance and accountability. They are the foundation upon which a successful organizational culture is built. If management sets, demonstrates and enforces high standards for performance and accountability, there is a strong likelihood that the organization will follow. And, longevity is a key ingredient. For example, Daniel S. Goldin, Administrator of the National Aeronautics and Space Administration (NASA), was named to his post in the spring of 1992. Goldin has won considerable acclaim for demanding nothing but the best from his employees, and thereby turning around a bureaucracy that had become ossified and recalcitrant to higher authority, including the President. He did not do it overnight, though. His "watch" is now seven years long and still going. By contrast, the average stay for an Energy Secretary has been about two and a half years; a Deputy Secretary, less than two years; and an Under Secretary, less than 18 months.[1]

CLARITY OF MISSION

Employees must know who they are and why they are there. Mission statements may seem corny to some, but from our experience good ones work. NASA's is crisp, clear and bold: "NASA is an investment in America's future. As explorers, pioneers and innovators, we boldly expand frontiers in air and space to inspire and serve America, and to benefit the quality of life on Earth." The Energy Department also declares itself a department of the future; it's slogan is "Science, Security and Energy: Powering the 21st Century." However, we wonder if the DOE employees in the field really have a sense of purpose and direction. Those at the Oakland Operations Office are challenged to, "serve the public by executing

programs and performing DOE contract management." At Albuquerque Operations Office, the rallying cry is, "to contribute to the welfare of the nation by providing field-level federal management to assure effective, efficient, safe and secure accomplishment of the Department's national defense, environmental quality, science and technology, technology transfer and commercialization and national energy objectives."[2]

DEDICATION TO EXCELLENCE

It is the responsibility of leadership to emphasize continuously and top-to-bottom the absolute importance of quality of performance. People truly dedicated to excellence usually achieve it.

EMPHASIS ON CORE COMPETENCIES

Those agencies that constantly emphasize the business areas in which they must absolutely excel, usually do so. At NASA, we are told, rarely, if ever, does the Administrator give a speech in which safety is not emphasized. DOE has appropriately emphasized excellence in the quality of its scientific and technical work, but only recently has begun to emphasize security, and only in recent months has articulated the importance of counterintelligence. The panel was hard pressed to find either words mentioned in speeches by most of Secretary Richardson's predecessors.

MINIMAL POLITICAL PRESSURES

Blessed is the government manager whose operations fall into only a handful of Congressional districts and under the purview of only a couple of oversight committees. It doesn't take a nuclear scientist to understand that the more Congressional districts and committees with which a federal agency must contend, the more it is politically whip–sawed in its priorities and stuffed with pork. We suspect the Department of Energy probably holds some federal records: its multitudinous and widely cast operations come under the scrutiny of no less than 18 Congressional committees and fund well-paying federal and contractor jobs in more than 50 congressional districts.

STREAMLINED FIELD OPERATIONS

In just about any endeavor, but especially in managing government contracts, simpler is better. Managing government contracts has become a major function in more and more agencies and departments as they seek to cut costs. We know of a few good examples of agencies where this effort is both efficient and effective.

One is the National Reconnaissance Office (NRO), a semi-autonomous Defense Department agency, which has long managed huge contracts with major industrial firms that have built and help operate our nation's surveillance satellites. The NRO, however, came under heavy fire several years ago for budget irregularities, partly as a result of tangled lines of bureaucratic authority. Today, after some substantial streamlining, multi-million dollar contracts are run out of program management offices at NRO Headquarters on a line of accountability leading directly to the contracting company. Rather than maintaining large field offices, the NRO employs only a handful of representatives in the field—typically only one or two peo-

ple resident at their largest contractors. The rest is done from Washington. To manage their largest contracts, no more than 15 contracting officers—from worker–level to management—are involved. Some are worth several billion dollars. Currently, the NRO manages over 1,000 contracts worldwide, with a combined value numbering in the tens of billions of dollars. They manage these contracts using a staff of approximately 250 contract officers.[3]

Though we acknowledge that there are differences between the missions of NRO's satellite contractors and DOE's nuclear weapons lab contractors, we are stunned by the huge numbers of DOE employees involved in overseeing a weapons lab contract. For example, Sandia National Weapons Laboratory, a contractor–operated facility in New Mexico, has several layers of Energy Department employees with whom it must deal: the Kirtland (Air Force Base) Area Office, with about 55 "feds," which is subordinate to the Albuquerque Field Office (AFO), which has a total complement of about 1,300 government workers. Albuquerque also monitors contracts with Los Alamos National Lab (through a Los Alamos Area Office of some 70 people), and several other contractors throughout the southern United States. Notably, Albuquerque is but one of 11 such DOE Field Offices, that boast a total field complement of about 6,000. Back at DOE Headquarters, which has a total work force of close to 5,000, Sandia's contracts are monitored, depending on the subject, by several Program Offices—including Defense Programs (somewhat over 100 officials) and Environmental Management (somewhat over 200 officials).

We repeatedly heard from officials at various levels of DOE and the weapons labs how this convoluted and bloated management structure has constantly transmitted confusing and often contradictory mandates to the labs. This is vividly illustrated by the labyrinthine organizational charts that one must decipher to trace lines of authority.

RESPONSIBILITY AND ACCOUNTABILITY IN SECURITY

One senior CIA official told us that the NRO security system is the best in the government—a view echoed, we understand, in a forthcoming report by the DCI/Defense Secretary Joint Security Commission. One can see why. At the NRO, security starts at the top. The chief of security provides policy guidance and monitors implementation. However, from the Director on down, all line managers are responsible for implementation. If a security breach occurs, the Director and appropriate line subordinates all are accountable. Similarly, NRO contractors are expected to meet fully NRO security standards and guidelines. Failure to meet those guidelines could well result in forfeiture of performance award fees, at the least.

FULL OPERATIONAL INTEGRATION

To be effective, security must be more than a concept, it must be woven into every aspect of the agency's business and the daily work of every employee. The NRO integrates security more fully than most other federal agencies we have seen. Though it has separate line items for security and counterintelligence functions, most security–related expenditures are integrated directly into the line items of every satellite program. Thus, rather than imposing security mandates as contract "add-ons," security officials work with the NRO managers to

fold their requirements into a given program during the planning stages. In this structure, security requirements are as much a part of an NRO satellite program as are solar cells and thrusters. And, the NRO security professionals, rather than treated as staff functionaries, are accepted as true partners in the NRO mission.

A PREVAILING CONSCIOUSNESS

Making people aware is vital. The record clearly shows that DOE has had mixed results from its various security and counterintelligence indoctrination programs. Briefings, town hall meetings and educational films are helpful, but they cannot take the place of a working environment in which security is just part of the daily routine. Again at the NRO, when a management decision is made, security always gets a voice. A security official is present at every level of NRO decision making: from the Office Director, to his Board of Directors, to the management teams of the smallest NRO program, security officials are part of the management process. Moreover, "security" gets a vote equal to that of any program manager. From the record, we judge that security at DOE, until recently, only occasionally had a voice; and when it did, many managers vociferously objected. Counterintelligence, on the other hand, was allowed little more than a whisper.

RESTRUCTURING

The panel is convinced that real and lasting security and counterintelligence reform at the weapons labs is simply unworkable within DOE's current structure and culture. To achieve the kind of protection that these sensitive labs must have, they and their functions must have their own autonomous operational structure free of all the other obligations imposed by DOE management. ***We strongly believe that this cleaving can best be achieved by constituting a new government agency that is far more mission–focused and bureaucratically streamlined than its antecedent, and devoted principally to nuclear weapons and national security matters.***

The agency can be constructed in one of two ways. It could remain an element of DOE but become semi-autonomous—by that we mean strictly segregated from the rest of the department. This would be accomplished by having the agency director report only to the Secretary of Energy. The agency directorship also could be "dual-hatted" as an Under Secretary, thereby investing it with extra bureaucratic clout both inside and outside the department.

We believe there are several good models for this course of action: the National Security Agency and the Defense Advanced Research Projects Agency, both elements of the Defense Department; and the National Oceanographic and Atmospheric Administration, an agency of the Commerce Department. Alternatively, the agency could be completely independent, with its administrator reporting directly to the President. The National Aeronautics and Space Administration and the National Science Foundation are also good models.

Regardless of the mold in which this agency is cast, it must have staffing and support functions that are autonomous from the remaining operations at DOE. These functions, which report directly to the Director, must include: an inspector general; a general counsel; a

human resources staff; a comptroller; a senior official responsible solely for security policy, and another responsible solely for counterintelligence policy. To protect its autonomy and avoid the diversion of funds to other purposes, the agency budget must be a separate line item strictly segregated by Congress from other budget pressures—even if it remains nominally within the current DOE structure. The agency also must have a separate employee career service. The panel recommends an "excepted service" model of employment, like many of the intelligence community elements, which would facilitate accountability and higher performance levels by allowing management to reward, punish, hire, and fire employees more easily.

To ensure its long–term success, this new agency must be established by statute. That statute, moreover, must clearly stipulate that nothing less than an act of Congress can amend the agency's mission, functions or affiliations. Clearly, Congress and the President must decide definitively which of these two solutions to enact. The panel has no specific preference between them; we believe either can be made effective. Should Congress and the President conclude that retaining the agency inside DOE is not workable, the "wholly-independent" approach should be enacted.

We emphasize that it is very important for the new structure to be organized to preserve and, if possible, enhance the ability of the national weapons labs to attract and retain scientists of the highest caliber. Excellence in the caliber of the scientists and their research and development programs must be sustained if the weapons labs are to fulfill their missions in the front line of U.S. national security. To meet this goal, continued but carefully controlled interaction with foreign visitors and scientists from around the world as well as with researchers from DOE's nondefense labs is essential for producing the best science. In the semi-autonomous model, the Secretary would be responsible for managing and ensuring the effectiveness of agency relations with the nonweapons labs.

Whichever solution Congress enacts, we do feel strongly that the new agency never should be subordinated to the Defense Department. Defense already is populated with a number of semi–autonomous agencies; we see no reason to add to that burden. Moreover, we believe the decision made long ago to house America's nuclear weapons research and development in a civilian government agency still makes sense. ***Specifically, we recommend that the Congress pass and the President sign legislation that:***

- ***Creates a new, semi–autonomous Agency for Nuclear Stewardship (ANS), whose Director will report directly to the Secretary of Energy.*** The Director should be dual–hatted as an Under Secretary of Energy. This new agency will oversee all nuclear weapons–related matters previously housed in DOE, including Defense Programs and Nuclear Nonproliferation; it also will oversee all functions of the National Weapons labs. (If Congress opts to create a totally independent agency, the Director should report directly to the President.)

- ***Streamlines the ANS/Weapons Lab management structure by abolishing ties between the weapons labs and all DOE regional, field and site offices, and all con-***

tractor intermediaries. The so–called "GOCO," or "government owned, contractor operated," concept of lab management should be retained. GOCO has been very successful, particularly in providing employment conditions that attract scientists of the highest caliber, and the federal government is strongly committed to maintaining that working relationship. Even if DOE opts to retain these field entities for other purposes, the ANS should sever all association with them. All ANS/Weapons Lab communications and business should be handled by ANS Liaison Offices established in each lab and manned with a small staff. (Our short review time did not permit us to explore fully this issue. We doubt that any amount of time would be sufficient. Suffice it to say that we did learn enough about the costs and benefits of these myriad DOE field bureaucracies to persuade us to recommend cutting all ties between them and the new agency.)

- ***Mandates that the Director/ANS be appointed by the President with the consent of the Senate*** and, ideally, have an extensive background in national security, organizational management, and appropriate technical fields. Admittedly, finding an individual with solid credentials in all three areas may prove an elusive goal. However, meeting two out of those three criteria should be considered mandatory, provided that one of the criteria always met is management experience. The Deputy Director should have a background in an area that compensates for areas in which the Director lacks experience. The Director should serve for a minimum fixed term of 5 years, not coincident with quadrennial transitions of administrations, and be subject to removal only by Presidential direction.

- ***Stems the historical "revolving door" and management expertise problems at DOE*** by severely circumscribing the number of political appointees assigned to ANS and requiring all ANS senior political appointees to have strong backgrounds in both national security (intelligence, defense, or foreign policy) and management (corporate, government, or military).

- ***Ensures effective administration of safeguards, security, and counterintelligence at all the weapons labs and plants by creating a coherent security/CI structure within the new agency***. We strongly recommend following the NRO's model of security management. The senior CI official at ANS—we recommend a Special Assistant to the Director for CI policy—should be mandated as a permanent FBI senior executive service position.

- ***Abolishes the Office of Energy Intelligence.*** A Special Assistant to the ANS Director for Intelligence Liaison should be created within the new agency, with a staff of no more than 20. The Special Assistant should be responsible for managing relations with the intelligence community, briefing ANS senior management on intelligence matters, and ensuring ANS intelligence requirements are met. This office should follow the Treasury Department model. (The Secretary of Energy would not be precluded from establishing a similar special assistant to address the department's non-weapons–related intelligence coordination and briefing needs.)

- Shifts the balance of analytic billets from the former Office of Energy Intelligence (about 40) to the DCI's Nonproliferation Center to bolster intelligence community technical expertise on nuclear matters. These billets should be permanently funded by ANS, but permanently assigned to the DCI Center. Weapons lab employees and ANS civil servants should be temporarily assigned to these positions for two year tours.

A Semi-Autonomous or Wholly Independent Nuclear Weapons Stewardship Agency should have the following attributes:

- The agency would be entirely separated from DOE, except in the semi-autonomous case, where the agency director—as a DOE Under Secretary—would report directly to the Secretary.

- The agency would have no other bureaucratic ties to DOE, other than R&D contracting, which would be managed by the agency Deputy Director. The weapons labs would be encouraged nonetheless to foster strong scientific interactions with the other DOE research labs. In the case of a wholly independent agency, the Director would be the chief executive officer.

- In the case of a semi-autonomous agency, the Director would be dual-hatted as a DOE Under Secretary.

- An independent oversight board would monitor performance and compliance to agency policies and guidelines, up and down the organizational structure.

- Authority from the agency Director to the weapons labs would run directly through the Deputy Director, who also would be dual-hatted as the Defense Programs Manager and, therefore, a manager of lab work.

- The security chief, directly reporting to the agency Director, would promulgate all security policies and guidelines for the agency and the weapons labs, including safeguards and cyber-security.

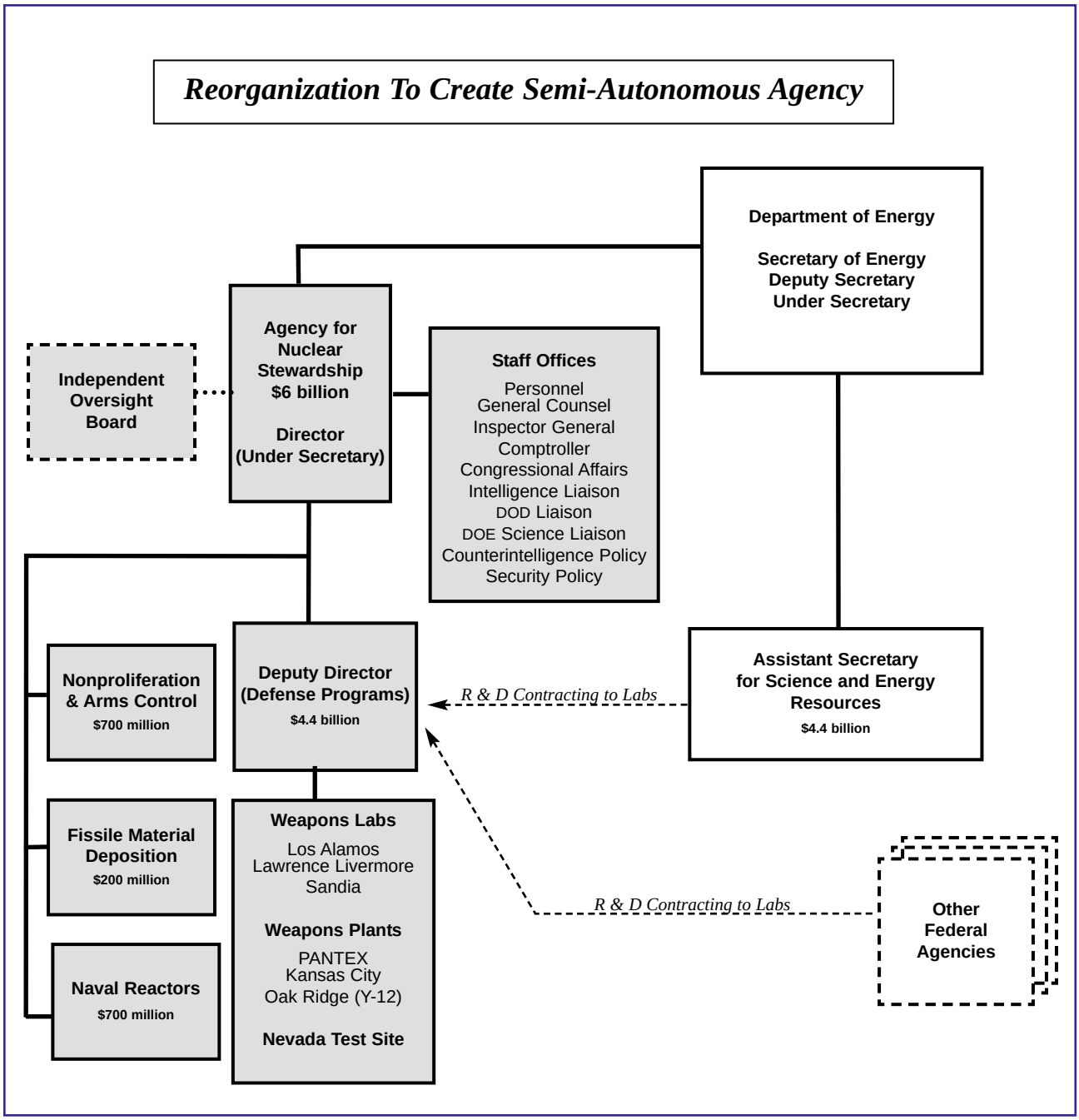
- The counterintelligence chief, also directly attached to the agency Director, would promulgate all counterintelligence policies and guidelines for the agency and the weapons labs. He/she also would manage the foreign visitors and assignments program.

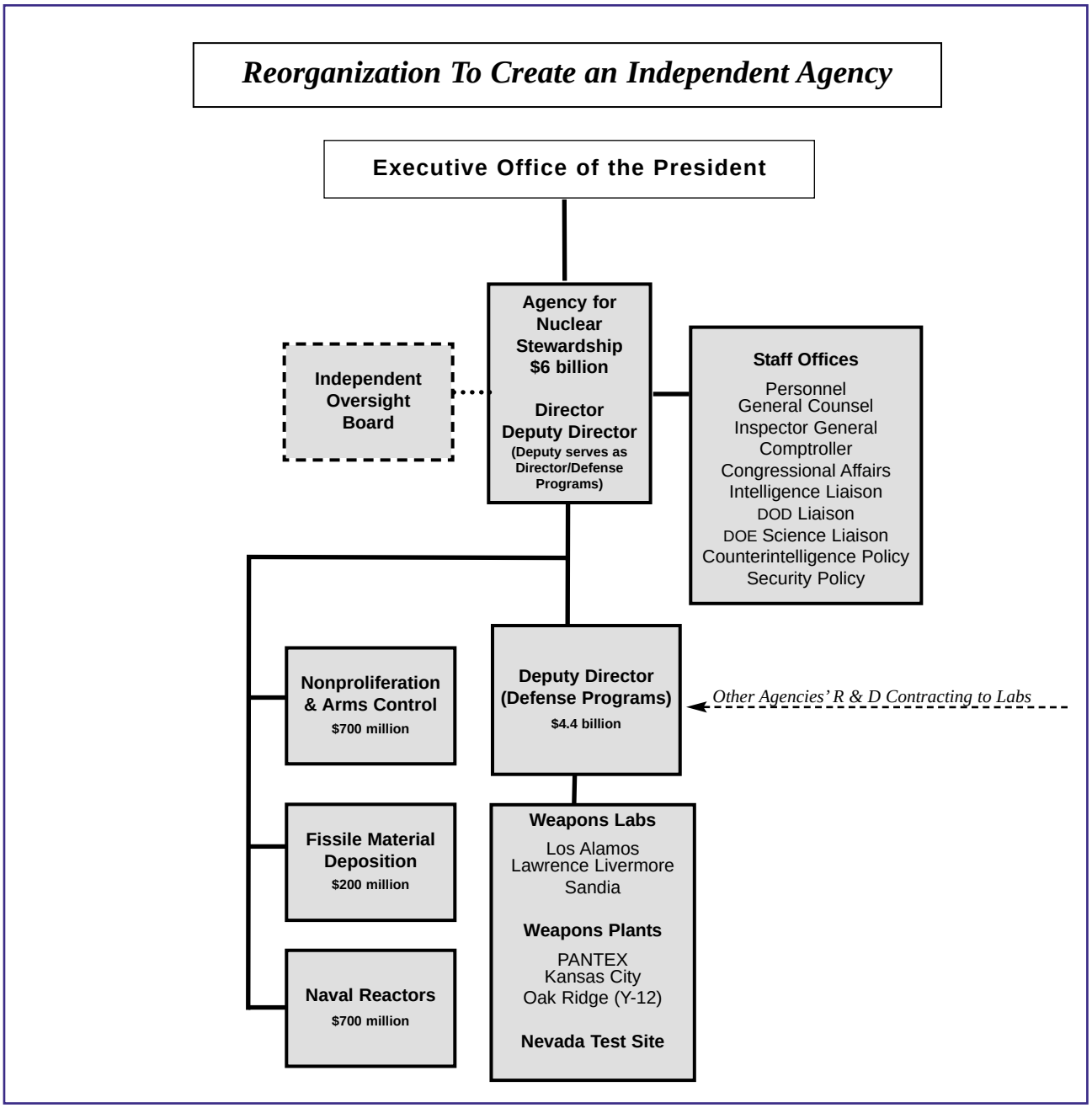
- As Defense Programs Manager for the weapons labs, the agency Deputy Director would be responsible for ensuring the integration of all security and counterintelligence policies and guidelines into all weapons lab programs.

- Security officers and counterintelligence officers would be attached to all line offices,

with heavy representation in Defense Programs, where full integration would occur. They also would be attached to all labs, in multiple numbers.

- Security and counterintelligence officers would report to their appropriate line managers on a day-to-day basis, but also report respectively to the agency security and counterintelligence chiefs on policy implementation issues. All policy implementation disputes would be referred back to the agency director for resolution.




Reorganization To Create an Independent Agency
Executive Office of the President
Agency for Nuclear Stewardship $6 billion
Director
Deputy Director
(Deputy serves as Director/Defense Programs)
Independent Oversight Board
Staff Offices
Personnel
General Counsel
Inspector General
Comptroller
Congressional Affairs
Intelligence Liaison
DOD Liaison
DOE Science Liaison
Counterintelligence Policy
Security Policy
Nonproliferation & Arms Control
$700 million
Deputy Director (Defense Programs)
$4.4 billion
Other Agencies' R & D Contracting to Labs
Fissile Material Deposition
$200 million
Naval Reactors
$700 million
Weapons Labs
Los Alamos
Lawrence Livermore
Sandia
Weapons Plants
PANTEX
Kansas City
Oak Ridge (Y-12)
Nevada Test Site

ADDITIONAL RECOMMENDATIONS

There are a number of initiatives that must be undertaken immediately to start building a new agency culture and identity and restoring public confidence:

- Establish a clear mission and clear standards of excellence. The agency's mission, and that each subordinate unit, must be clearly articulated. Strong security and counterintelligence in addition to scientific achievement must be core elements of the mission. Similarly, clear standards of excellence must be established throughout the organization. Excellence must be the goal of scientists, engineers, technicians, and managers as well as security and counterintelligence officials.

- Establish a clear chain of accountability. There must be clear, simple, indelible lines of accountability from top to bottom. If a failure occurs, there must be a straightforward means for determining accountability—at all levels. Seeking consensus and advice is important, but ultimately a decision must be made by individuals, and those individuals should be held accountable.

- Hold leaders accountable. Accountability must be enforced, particularly among the agency managers who will form the backbone of the new agency and instill a new culture of excellence.

- Reward achievement. Criteria should be clear and rewards substantial. Protection of nuclear secrets and expansion of scientific knowledge should be among the most valued. Achievement must be judged on contribution to mission, not to program expansions or budget increases.

- Punish failure ... with severity, if necessary. Penalties should be tough, but fair and proportional. Laxity in protecting nuclear secrets and other sensitive information should be among the most severely punished.

- Train and educate. Establish a formal educational and training system to develop a professional cadre of career managers and leaders. Security and counterintelligence should be major parts of the core curriculum passed down to all lab personnel in regular briefings and training sessions.

- Do not forget the primary mission. Preserve and strengthen those agency attributes—including cutting edge research in the most advanced scientific

fields—that will attract the finest talent in the nation. With respect to the weapons laboratories, continue to foster their unparalleled lead in intellectual excellence. But never lose sight that protecting the nation by securing its nuclear stockpile and nuclear secrets—through good science and good management—is Job Number One.

- While maintaining its autonomy, the agency should nonetheless emphasize continued close scientific interaction with the DOE research labs not engaged in weapons–related endeavors. In the semi–autonomous alternative, DOE should also be responsible for ensuring that good relations are maintained between the non-weapons labs and the weapons labs.

SECURITY AND COUNTERINTELLIGENCE ACCOUNTABILITY

- Accountability. The agency director should issue clear security accountability guidelines. 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.

- Independent Oversight. 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.

- Joint Committee for Congressional Oversight of ANS/Labs. Congress should abolish its current oversight system for the national weapons labs. Just as the profligate morass of DOE contractors and bureaucrats has frustrated the critical national interest of safeguarding our nuclear stockpile, so has the current scheme of Congressional oversight with roughly 15 competing committees laying claim to some piece of the nuclear weapons mission.

- ANS Inspector General. The President, Congress, and the director of the new agency should cooperatively, through executive order, legislation, and agency directive, provide teeth to the authority of the new agency's inspector general. For example, the inspector general, the independent oversight body, and the agency director should all have to concur on the findings of the annual report to the President on safeguards and security at the weapons labs.

EXTERNAL RELATIONS

- The CIA and FBI should expand their "National Security Partnership" to include the new agency and the weapons labs. Reciprocal assignment programs should be implemented to promote cross-fertilization of expertise and experience.

- CIA and DIA should bolster their support for ANS needs. Both intelligence agencies should establish analytic accounts to support the specific substantive and counterintelligence interests and needs of the new ANS and the weapons labs. These accounts, among other issues, should regularly produce data on the nuclear–related collection efforts of all foreign governments and foreign intelligence services. This data should serve as the foundation for regularized weapons lab counterintelligence briefs for the foreign visits/foreign visitors programs.

- Improve national security and law enforcement cooperation, particularly with respect to counterintelligence case referrals and handling. The National Security Council should take the lead in establishing clear Executive Branch guidelines and procedures for resolving disputes between agencies over law enforcement and national security concerns. A government–wide process needs to be established by which competing interests can be adjudicated by officials who are properly informed of all relevant facts and circumstances, but who also are sufficiently senior to make decisions stick.

- Ensure a government–wide review of legal tools to address the current foreign intelligence threat. The National Security Council should conduct a review to ensure that sufficient legal authority and techniques are available and appropriate in light of the evolution of a very sophisticated threat and the ongoing revolution in information systems.

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 all contract employees clearance requirements. 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. Promulgate new agency guidelines and standards for security–related administrative inquiries to ensure that proper security/counterintelligence procedures and methods are employed. Very high profession-

al qualification standards should be established and strictly maintained for all security personnel involved in administrative inquiries.

PHYSICAL/TECHNICAL/CYBERSECURITY

- Comprehensive weapons lab cyber–security 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 U.S. 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. A "best practices" review should be conducted yearly by the appropriate agency security authority.

- Comprehensive classified document control system. Document controls for the most sensitive data of the weapons labs should be reinstituted by the agency Director. The program should be constantly monitored by a centralized agency authority to ensure compliance.

- A 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 secrets are 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 nearby the weapons labs. The panel offers additional thoughts for improving the Department's CI efforts in the Classified Appendix to this report.

ENDNOTES

CHAPTER: ROOT CAUSES

[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] Boyer, Paul. *By the Bomb's Early Light: American Thought and Culture at the Dawn of the Atomic Age.* Chapel Hill: University of North Carolina Press, 1985, p. 138.

[3] National Science Foundation, "Science and Engineering Indicators," 1996.

[4] National Science Foundation, "Data Brief," Vol. 1996, No. 9, August 19, 1999.

[5] Classified report.

[6] Classified DOE Report.

[7] DOE, "Annual Report to Congress, 1978," April 1979.

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

CHAPTER: RECURRING VULNERABILITIES

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

[2] Classified DOE Report.

[3] Classified DOE Report.

[4] Classified DOE Report.

[5] Classified DOE Report.

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

[7] Classified U.S. Government report.

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

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

[10] Classified DOE report.

[11] DOE, “Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security,” February 1993

[12] Classified FBI document.

[13] Classified U.S. Government report.

[14] Classified DOE report.

[15] DOE, “Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993,” January 1994 (U)

[16] DOE/IG-385, “Special Audit Report on the Department of Energy’s Arms and Military-Type Equipment,” February 1, 1996

[17] Classified DOE report.

[18] DOE, “Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities,” September 1996

[19] 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,” December 13, 1991

[20] GAO/RCED-90-122, “Nuclear Security: DOE Oversight of Livermore’s Property Management System is Inadequate,” April 18, 1990

[21] 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), April 20, 1999

[22] 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), April 20, 1999

[23] Classified DOE report.

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

[25] GAO/RCED-89-34, “Nuclear Security: DOE Actions to Improve the Personnel Clearance Program,” November 9, 1988

[26] DOE/IG/WR-O-90-02, “Nevada Operations Office Oversight of Management and Operating Contractor Security Clearances,” March 1990;

[27] Classified DOE report.

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

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

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

[31] Classified U.S. Government report.

[32] Classified DOE report.

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

[34] Classified DOE report.

[35] Classified DOE report.

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

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

[38] Classified DOE report.

[39] Classified DOE report.

[40] Classified DOE report.

[41] Classified DOE report.

[42] Classified DOE report.

[43] *New York Times*, "Abstract," August 5, 1977

[44] DOE, "Plutonium: The First 50 Years. United States Plutonium Production, Acquisition, and Utilization from 1944 Through 1994

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

[46] GAO/RCED/AIMD-95-5, "Nuclear Nonproliferation: U.S. International Nuclear Materials Tracking Capabilities are Limited," December 27, 1994

[47] GAO/AIMD-95-165, "Department of Energy: Poor Management of Nuclear Materials Tracking Capabilities Are Limited," August 3, 1995

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

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

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

[51] Classified U.S. Goverment report.

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

[53] Classified DOE report.

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

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

[56] DOE, "Response to the Cox Committee Report: The Benefits of Department of Energy International Scientific and Technical Exchange Programs," April 1999.

[57] GAO/RCED-99-19, "Department of Energy: Problems in DOE's Foreign Visitors Program Persist," October 6, 1998.

CHAPTER: ASSESSMENTS

[1] 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.

[2] 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.

CHAPTER: REORGANIZATION

[1] DOE, "Department of Energy First Tier Organizations, Terms of Office," undated.

[2] DOE, Field Fact Book, May 1998.

[3] Unclassified organizational data provided by National Reconnaissance Office.