Union Calendar No. 386

106TH CONGRESS, *2d Session* | HOUSE OF REPRESENTATIVES | REPORT 106–687

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

REPORT

OF THE

REDMOND PANEL

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

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

---

U.S. GOVERNMENT PRINTING OFFICE

79–006 WASHINGTON : 2000

LETTER OF TRANSMITTAL

PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC, June 21, 2000.

Hon. J. DENNIS HASTERT,
Speaker of the House,
U.S. Capitol, Washington, DC.

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

Sincerely yours,

PORTER J. GOSS,
Chairman.

Union Calendar No. 386

106TH CONGRESS, *2d Session* } HOUSE OF REPRESENTATIVES { REPORT 106–687

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

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

Mr. GOSS, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

EXECUTIVE SUMMARY

In the wake of last year's reports by the Cox Committee [1] on Chinese nuclear espionage and by the President's Foreign Intelligence Advisory Board (PFIAB) on security lapses at the Department of Energy's (DOE's) nuclear weapons laboratories, and in response to Presidential Decision Directive NSC 61 (PDD–61),[2] Secretary of Energy Bill Richardson embarked on a comprehensive reform of counterintelligence (CI) at DOE. This was accelerated and significantly refined in response to legislation proposed by Congress which, among other things, created the National Nuclear Security Agency (NNSA).

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

[1] The Cox Committee's formal name was the House Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China.

[2] PDD–61 was issued on February 11, 1998 in response to reports from the General Accounting Office and from the Intelligence Community that derided CI and security at DOE and its constituent laboratories.

CI and a former head of CI at the Central Intelligence Agency (CIA).

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

Among the specific findings and recommendations from the review are:

- The current director of CI at DOE is an excellent choice for the job. Moreover, he has access to and the support of the Secretary.
- DOE has failed to gain even a modicum of acceptance of the polygraph program in the laboratories. DOE must involve laboratory management in deciding who will be polygraphed.
- DOE's efforts to improve CI awareness training have failed dismally. In developing its CI awareness training program, DOE should draw on the positive experience of other U.S. government agencies, in particular the CIA and National Security Agency (NSA).
- DOE also faces a considerable challenge in the area of cyber CI, that is, protecting classified and sensitive computerized media databases and communications from hostile penetration. This will require significant investment in defenses and countermeasures and require the assistance of other federal agencies.
- DOE CI has established an excellent, well-staffed, and effective annual CI inspection program that will serve to ensure the maintenance of CI standards and continued improvements in the program.
- The "shock therapy" of suspending the foreign visitor and assignment programs worked in making the laboratories realize the degree to which these programs, if not properly managed, can be a counterintelligence threat. The CI components at the laboratories now appear to be better involved in the process of granting approvals for visits and assignees.
- Cooperation at each laboratory between CI and security personnel is largely informal and dependent upon personal relationships. DOE and the laboratories must establish more formal mechanisms to ensure effective communication, coordination, and, most importantly, the sharing of information.
- The CI offices at the laboratories are hampered by their not being cleared for access to certain Special Access Programs (SAPs). Thus, the CI components are unable to exercise CI oversight of these activities. The Director of Central Intelligence (DCI) should work with the DOE Secretary to remedy this situation.
- DOE needs to establish contractual CI performance standards for the laboratories against which they can be judged and duly rewarded or penalized.
- It should be noted that the Committee has not adopted the Redmond Panel's position in favor of the maintenance of the

current centralization of all CI authority at DOE for a short, transitional period.

Introduction and scope of investigation

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

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

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

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

The team notes that DOE was not unique in de-emphasizing basic security procedures in the wake of the end of the Cold War. The State Department, for example, embarked on its now infamous

"no escort" policy, the Defense Intelligence Agency issued "no escort" badges to Russian military intelligence officers, and even the Central Intelligence Agency precipitously abandoned its policy of aggressively recruiting Russian intelligence officers. The present and future Administrations must ensure that such laxity will never again be encouraged or tolerated.

DOE Office of Counterintelligence (DOE CI)

Presidential Decision Directive NSC 61 (PDD 61), issued on February 11, 1998, provided for the establishment of a new DOE CI program that reports directly to the Secretary of Energy. In April 1998, DOE's CI office became operational. Under the guidance of the director of DOE CI, Mr. Edward Curran, the Department has made considerable progress towards establishing an effective CI operational capability at DOE Headquarters to do the analytical and investigative work necessary to identify and neutralize insider penetrations. It is the team's opinion that Mr. Curran is ideal for the CI director job because of his extensive CI experience at the FBI, his rotational assignment at the CIA, and his persistence and determination.

Mr. Curran appears to have access to and the support of the Secretary of Energy, which is an essential ingredient to an effective CI program. Moreover, he is vigorously attempting to exert DOE CI authority and influence over the laboratories, which, while difficult to accomplish, is critical to the success of the new CI program. In the future, direct access to the Secretary and close working relations with other offices reporting directly to the Secretary, including the Offices of Security Affairs and Intelligence, will be crucial. In addition, DOE CI must establish and maintain a mutually supportive relationship with the Office of Independent Oversight and Performance Assurance, which performs inspections of DOE programs and policies. This office has an established record [3] of detecting, documenting and reporting CI and security shortcomings at the laboratories. Regrettably, past findings of this office in the CI realm evidently were rarely acted upon. This office, which is philosophically attuned to CI and security issues, now has a good working relationship with DOE CI and has recently pointed out at least one CI cyber security [4] vulnerability. In the future, the office will be a natural ally for DOE CI as it tries to assert authority, identify problems and implement new policies.

Mr. Curran is hiring and, where necessary, training a good cadre of CI officers to perform investigations from DOE Headquarters. The CI components at the laboratories,[5] moreover, seem well on the way towards adequate staffing. Laboratory interaction with the FBI appears to be effective, at both the management and CI component level. That said, laboratory CI offices will need to focus for the foreseeable future on (1) gaining the confidence of their laboratory colleagues; (2) crafting CI programs that fit the unique needs

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

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

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

of each lab; and (3) conforming to DOE's requirements for more standardized approaches and procedures. The team appreciates that the job of reforming CI at DOE and the laboratories will require steadfast resolve on the part of Mr. Curran and his successors, continued support from the Secretary, and sustained resources from Congress.

Congressionally mandated reorganization of DOE

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

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

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

Separation of CI and security disciplines at the laboratory level

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

Such claims notwithstanding, the team discovered that these "multiple-neuron-type" arrangements are not formalized in any meaningful way at any of the three laboratories. In each case, the communications arrangements appear to depend primarily on personal and working level relationships. It has been the sad experience in many espionage cases that only after the spy is uncovered, does it become clear that a plethora of counterintelligence indicators concerning various facets of the individual's life, performance,

and behavior, had been known in different places by different individuals, but never effectively collated or holistically evaluated.

DOE must ensure that the CI officers at the laboratories are part of a formal system set up locally to ensure that all relevant CI and security data information is collected, assembled, and analyzed by means that are not solely dependent on personal relationships. Otherwise, the retirement or transfer of one individual in the process could cause the whole system to break down. Without an effective organizational structure, there is no guarantee that all relevant data will become known to the CI office. The team is not satisfied that DOE and the laboratories have completely grasped this concept. Moreover, the DOE Operational Field offices at Albuquerque and Oakland continue to refuse to share relevant information from employee personnel files under their control with DOE CI or laboratory CI components. The team learned that DOE CI is not even informed by these three offices when an employee loses his or her security clearance. Therefore, the team recommends that DOE ensure that a formal communications process for CI information between and within the laboratories and between DOE Operational Field offices and CI personnel be established immediately.

CI inspection teams

PDD–61 requires an annual inspection of DOE's CI program. DOE CI has hired and deployed a dozen retired FBI, CIA, and military intelligence officers to inspect the CI programs at the three weapons laboratories. This excellent initiative is already yielding promising results by identifying systemic problems and offering solutions. The inspection team consists of highly experienced individuals, who appear to be insulated from the politicization that can yield watered down findings. The team's effectiveness, however, will be largely dependent upon the frequency of its inspections. We recommend that DOE continue annual inspections as stipulated in PDD–61 and add follow-up inspections focusing on specific problem areas. The team judges that there is no DOE CI program that is more useful or efficient than this inspection regime. We recommend, therefore, that resources adequate to expand this inspection program be provided.

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

Polygraph testing

Polygraph testing for "covered"[6] DOE and laboratory personnel was mandated by Congress, but DOE Headquarters reacted with poorly thought out and inconsistent directions to implement the requirement. As a result, laboratory personnel have a very negative attitude towards the polygraph. Moreover, since the polygraph is a highly visible part of the overall CI effort, the entire CI program has been negatively affected by this development. At the center of this problem is DOE's lack of success in explaining the importance and utility of the polygraph program. Further exacerbating this problem, DOE Headquarters personnel made little effort to consider the views of senior laboratory managers and have not involved them in the planning process for determining who will be polygraphed. In addition, DOE Headquarters efforts to meet with the laboratory employees to explain the polygraph program have been ineffective, if not counterproductive. To make matters even worse, DOE Headquarters, by vacillating and changing the policy over time, appeared inconsistent and unsure where the opposite is essential to instill confidence in the program parameters and professionalism.

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

In addition to the emotional reactions, there are rational questions about the polygraph, such as, "What are they going to do with the inevitable number of people who do not pass?" The team shares this concern, and expects that there will be a significant number of so-called "false-positive" polygraph results that will have to be further examined. Another concern voiced to the team by numerous laboratory employees was that "No one has ever tried this before on this scale." The fact is that never before have so many "cleared" employees of a government organization had to have their clearances (and, thus, their livelihoods) threatened by the institution of the polygraph.

Compounding the problem further is an attitude among many laboratory employees that they are indispensable and special, and

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

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

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

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

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

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

Counterintelligence awareness training

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

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

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

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

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

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

THE VIEW FROM THE LABORATORIES

Laboratory management made the following comments regarding training and awareness:

- "Some of the awareness training material received from Washington is so bad it is embarrassing. Were it used, it would undermine the credibility of the whole program."
- "We had to scramble to find speakers on the subject [of CI during a lab-wide CI and security stand-down]."
- "One [CI] lecture given by an experienced former FBI agent, tailored to the laboratory audience, was a huge success. We need more of this sort of thing."
- "There is no line budget item for training, each speaker costs about $4,000, yet there is no Headquarters-generated program."
- "DOE Headquarters' approach to training and awareness has been form over substance, represented by dictated programs and policies."

- "There is an acute need for 'realistic' awareness training, so people will realize the problem did not go away with the Cold War and they are still targets."
- "There are [laboratory] divisions standing in line for tailored presentations."
- "Concrete examples, real [CI] incidents, and their consequences are required to get people's attention. They [the scientists] must be captured intellectually."

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

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

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

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

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

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

Cyber CI

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

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

There has existed for years at the laboratories an entity called the Computer Incident Advisory Capability (CIAC) that was responsible for collecting and analyzing computer security incident data. The reporting to this organization has historically been voluntary, and anonymity was permitted to encourage the laboratories to be frank and forthcoming. More recently, the CIAC has begun to provide DOE Headquarters with intrusion incident summaries.

The lack of specificity in these summaries, however, makes meaningful analysis impossible. DOE CI, with assistance and support from DOE management, needs to assert its authority in this matter.

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

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

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

Foreign visits and assignments

The team limited its examination of this issue to the role played by DOE CI and the laboratory CI offices in the visitor and assignments approval process, which would lead to the laboratory director seeking a "waiver" to the moratorium on foreign visits from sensitive countries. The team notes that Secretary Richardson announced in December 1999 that he might start seeking such waivers as permitted by the FY 2000 National Defense Authorization Act.[7] All three laboratory CI chiefs stated that they now have an established, integrated role in the approval process leading to a laboratory director seeking a waiver to allow such a visit. For instance, the CI chief at Lawrence Livermore is one of four officers who must sign off before a request goes to the laboratory director for a decision to seek a waiver. The CI chief at Sandia is a member of the Foreign Visits and Assignments Team, which actually controls the approval process. These officials can thus bring to bear a CI perspective on any proposed visit, which the team believes to be a crucial function.

Obviously, the judgments made by the laboratory CI offices are only as good as data on which they are based. These data includes indices checks, which have often been slow in coming from other Federal agencies. The laboratory CI offices need to have access to broader-based intelligence information. This information, when integrated by the analysts in the CI offices, would give them a much improved basis on which to judge the CI threat that individual visitors and delegations might pose. Access to this information is prob-

[7] Washington Post, December 3, 1999 "Energy Chief to Allow Foreign Scientist to Visit Labs."

lematic, and DOE CI needs to work with other relevant entities at DOE Headquarters—particularly the Office of Intelligence—to arrange appropriate and efficient access in the field.

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

Apparently, the legislatively imposed moratorium on foreign visits and assignment has had the desired effect of making DOE and the laboratories much more conscious of the CI threat posed by visits.[8] Making the laboratory directors accountable has also had a salutary effect. It now remains for DOE CI and the laboratory CI offices to work together to make sure the CI role in the approval process is made as effective as possible by bringing to bear the maximum amount of data as efficiently as possible. There will also need to be more awareness training to sustain and better improve the presently enhanced levels of interest and attention.

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

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

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

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

tion prevails at Sandia, where it was evident that the CI component is often unaware of "Work-for-Others" activities.[9]

The net result of this situation at Lawrence Livermore and Sandia is that no one appears to be examining CI issues involving personnel engaged in the most sensitive SAPs and other Intelligence Community projects without a formalized reporting mechanism, there is no guarantee that an employee will report a CI incident to the contracting intelligence agency. The contracting agency, may or may not, in turn, report the problem or issue to the DOE Office of Intelligence, DOE CI, or to FBI Headquarters. The team judges this to be an unacceptable process for the transmission of such critical CI information. DOE Headquarters should reach a formal agreement with the Intelligence Community to ensure that the laboratory CI offices are read into the SAPs at least at an administrative level so they can fulfill their CI responsibilities. The team also encourages the Community Management Staff (CMS), which has been tasked by the Director of Central Intelligence (DCI) to examine the protection of Intelligence Community equities by DOE and the laboratories, to work closely with DOE to resolve this issue of the lack of a formalized reporting mechanism.

Sensitive unclassified technical information (SUTI)

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

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

In the team's judgment, DOE should proceed very cautiously and openly on SUTI imposition—if it does so at all—so as to avoid repeating the internal public relations mistakes it made with the

[9] Due to the communications arrangements between Los Alamos chiefs of intelligence, CI, and security, Los Alamos does not appear to have the same problem as the other two laboratories.

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

Enforcement

Each contract DOE has with the operators of the laboratories requires an annual appraisal of performance. In the past, these appraisals apparently included an ineffective pro forma consideration of security. It appears that neither DOE Headquarters nor DOE Field Offices, which are directly responsible for contract oversight, effectively enforced the terms of the contracts in this area. For example, the team was told that in some instances the University of California was not consciously aware of the fact that it was contractually responsible for certain security provisions, even though these were explicitly stated in the contract. The team recommends that DOE enforce existing security performance measures. Further, the team recommends that DOE incorporate measurable CI objectives and performance standards into each of its laboratory contracts. DOE could then use the previously mentioned CI audits, possibly combined with the findings of the Office of Independent Oversight and Performance Assurance, to evaluate the performance of the laboratories and impose penalties on the contractors for unacceptable performance.

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

Conclusions

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

DOE has not effectively laid the groundwork for acceptance of the polygraph program, an obviously essential part of any CI effort to detect and deter espionage by employees. Moreover, DOE has

failed to establish the absolutely key, complementary CI pillar—an effective training and awareness program.

No CI program can succeed unless both the operational and training pillars are in place and supporting each other. Further, it is clear from decades of behavior, that the DOE and laboratory culture is profoundly antithetical toward CI and security. Unless changed, this entrenched attitude will doom any attempts at long-term improvements. Effective training and awareness programs are the only way to change this culture.

DOE is just beginning to determine the magnitude of CI issues relating to the cyber threat, which includes e-mail and intrusions. The cyber component of DOE CI needs strong support at DOE Headquarters to establish suitable, minimum CI standards in systems controlled by DOE's information management units and the laboratories.

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

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

○