FPS NEWSLETTER JANUARY 2003 ARTICLES

Risk-Based Security at the National Labs: A Report of The Commission on Science and Security

AnneWitkowsky

Tension between science and security is not new, and it is not new at the Department of Energy laboratories. But, the turbulence that these laboratories experienced over the last several years, in the wake of the Wen Ho Lee investigation and the missing disk drives have put at risk the vitality of some of the nation's most valuable assets.

With the high-profile allegations and security violations at Los Alamos as a backdrop, Energy Secretary Bill Richardson chartered the Commission on Science and Security in October 2000 to assess the challenges facing DOE and the newly created National Nuclear Security Administration (NNSA) inside the DOE. Its charge was to examine how to maintain excellence in the conduct of science in the national laboratories while protecting and enhancing national security. The commission was asked to examine all DOE national laboratories (not just the three large nuclear weapons labs where classified work is most concentrated) in order to address the Department's broad range of classified and unclassified activities and information. That was because many of the newer security and counterintelligence measures deeply affected unclassified work and open science laboratories. The commission was comprised of 19 distinguished members from the scientific, defense, intelligence, law enforcement and academic communities. John Hamre, President and CEO of the Center for Strategic and International Studies (CSIS), chaired the commission and CSIS provided support to the Commission. In May 2002, the commission presented a final report to Secretary Abraham, who had re-chartered the commission after he took office.

The commission found that the context for its work was an environment where over the past two decades, the conduct of science and the security landscape have changed considerably. Some problems are long-standing in the structure and culture of the Department. At their core, they reflect the difficulties that the Department has had in making the transition from a world in which our national security laboratories were fairly insulated from the outside to one in which they have -- and need – much greater scientific interaction with other laboratories, institutions and industry. The nature of open science, in turn, has become much more international, collaborative, and networked. And these interactions are taking place in an environment in which the threats to our security have become more complex, multifaceted, and sophisticated, as our nation grapples with the war on terrorism and preventing weapons of mass destruction from falling into the wrong hands. Accordingly, providing for both excellence in science and security requires increased vigilance and threat awareness on the part of the national laboratories, within a risk-based security system that will allow open, unclassified scientific interaction to flourish.

The commission felt that the controversies following the Wen Ho Lee investigation and the investigation of the missing hard drives exacerbated many of the Department's existing problems. Well-intentioned, but poorly engineered, security procedures imposed in the wake of the security scandals were found to be undermining an atmosphere of creativity and innovation. This legacy deeply affects the open science community at the laboratories and ultimately will undercut not only DOE's science programs, but also our national security.

Summary of Analysis

The commission concluded that new approaches to improve security and counterintelligence must be developed, in a way that is complementary to the practice of science in the laboratories. Its report provides recommendations in five key areas that, if implemented, will provide a long-term strategy to help the Department of Energy meet its science and security goals. The commission's overarching finding was that the DOE's current policies and practices risk undermining its security and compromising its science and technology programs. In support of this finding, the commission identified five fundamental problems:

First, the commission found that the Department's continuing management dysfunction impairs its ability to carry out its science and security missions. Even the best security policies and sound processes for their development will not be effective if strong leadership and effective management are lacking. Many well-intentioned reform efforts, piled on top of a structure that traces back to the early days of the Manhattan Project, have created an organization with muddy lines of authority. The relationship between the Washington and regional offices of the Department, and the contractor-owned laboratories, create a complicated layered structure in which assigning accountability is difficult. Multiple constituencies mean that internal Department battles consume an inordinate amount of time and can be fought over and over repeatedly. As a consequence, the development and management of security policy lack clarity, consistency, and broad strategic planning.

Second, collaboration between the science community and security and counterintelligence elements has been badly damaged. The commission found no one from the scientific community who thought it was unimportant to protect national security information. Neither did it find anyone from the security community who felt laboratory scientists did not need to interact with outside peers. The commission did find widely differing views on what constitutes a significant risk to national security and how best to minimize those risks. There are deeply held differences dividing the communities over what requires protection, how much protection is needed, and by what means that protection should be provided.

Third, the commission found that DOE does not have an effective system for risk-based security management that encompasses the entire DOE complex. The Department lacks an approach for assessing risks to its assets that takes into account the entire DOE system. Thus, it does not have a means of comprehensively determining priorities for the protection of those assets. DOE also lacks a budget process that could support security decisions based on establishing risk and priorities. Therefore, spending on security overall is missing an underlying rationale, and cannot take into account the opportunity costs to science of implementing security measures. Additionally, the Department does not have the needed counterintelligence analytical capabilities to support and shape risk-based security management.

Fourth, the Department's investments in new tools and technologies for its security and counterintelligence programs are woefully inadequate. In the last few years, security and counterintelligence have received significant funding increases, but the commission found that virtually no resources were being devoted to develop systems that move beyond the Department's labor-intensive, paper-based security system. This lack of automation and

integration creates missed opportunities to significantly improve the monitoring of processes, facilities, and databases, and bogs down management and scientists under unnecessary administrative burdens.

Finally, the commission found that cyber security lacks sufficient priority in the Department. Management of DOE networks needs significant improvement. More than any other area, cyber security demands strong, smoothly functioning processes to ensure that the laboratories can protect themselves against cyber threats in a manner that is risk-based.

Summary of Recommendations

To make the necessary changes, the commission argued that the Department must establish a security and counterintelligence program that is sustainable for the long term — one that is risk-based and tailored to the missions and activities of the laboratories. Its report suggests five overarching sets of recommendations, summarized below.

1. Clarify Lines of Responsibility and Authority. First, if reforms in security and counterintelligence programs are to succeed, the Secretary and the Administrator of the National Nuclear Security Administration (NNSA) must address basic organizational problems at DOE, most significantly confusion over "line" and "staff" responsibilities. The commission recommends clarification of the chain of command between the Secretary and the laboratory directors; most important, that responsibility for security, like safety, or any other operational matter, must rest with line management. Together with a more clearly defined chain of command, DOE needs to reduce excess layers of management and staff that have built up within since the late 1980's. To support a more disciplined decision-making process on all matters, including security, the commission recommends that the Department install a rigorous multiyear budget process, modelled on the Planning, Programming, Budgeting, and System (PPBS) at the Department of Defense (DOD). Related to this point, the commission said that the idea of a separate security budget, administered by someone other than the laboratory director as the line manager, is a flawed concept, and recommended that line managers control the resources required to execute their missions.

2. Integrate Science and Security. DOE leadership must ensure that science and security at DOE is an integrated enterprise – collaborative and complementary. First, the commission underscored the importance of ensuring that laboratory directors have full responsibility and authority for science *and* security, and of holding them strictly accountable. The laboratory director must be chief scientist *and* chief security officer. Scientists and engineers throughout each laboratory must be invested in carrying out their missions securely, but this will only happen if laboratory directors themselves take a strong leadership role. Contracts, directives, and other guidance to the laboratories must reflect this philosophy; they must be performance-based so that laboratory directors have the capacity to implement them in a manner that is consistent with the work at their sites. At the same time, DOE oversight must be rigorous and DOE leadership must demand – and reward - accountability. To improve collaboration, the commission also recommended the creation of a high-level, Department-wide laboratory security council for the development of security policies. Its representation should include security, counterintelligence, the field offices, laboratory personnel, and others for whom security policy decisions will have a significant effect. The commission further recommended that laboratory directors establish comparable groups to integrate security decision-making and implementation at the site level. Together with these integration improvements, the commission said that DOE leadership must restore a climate

of trust within the Department, between managers at all levels, and between managers and employees.

3. Develop and Practice Risk-Based Security. Third, the Department must develop and practice risk-based security management. Risk-based security management is based on the premise that sensitive activities are not uniformly distributed throughout an organization and that assets representing a higher risk to national security require greater protection. A risk-based system should provide for the ability to make decisions about the marginal value (in an economist's definition, i.e., additional) of increasing investments in a given aspect of security, and the tradeoffs between security alternatives, as well as the tradeoffs between security and the science (programmatic) mission. The commission underscored that a modern security system must find a way to balance resources, which are limited, and risk, which can never be eliminated.

Specifically, the commission recommended the establishment of a risk-based systems approach to the development, analysis, and implementation of security policies throughout the DOE complex. A key to the success of this approach will be clear guidance for the laboratories about the Department's priorities for protecting its assets. That guidance can only be developed with the participation of national security, intelligence, and law enforcement agencies outside DOE. It also will require a greatly improved threat assessment process. The commission recommended that risk-based management plans be developed annually across security functions at each site. Specifically, in parallel with the fiscal budget, the Secretary and the NNSA Administrator should issue a single DOE-wide integrated safeguards and security plan that reflects the comprehensive plans agreed between the sites and federal managers.

To support this risk-based model, the commission found that the Department needs to strengthen, refocus and revalidate its counterintelligence program. It is crucial that DOE leadership expand the Department's counterintelligence analytical capabilities in order to conduct pattern analysis, monitor trends, and provide the threat assessments that are necessary for a security system that is properly oriented around risk. The commission recommended that the program broaden its cooperation and information access across agency boundaries, and, as discussed under "New Tools and Techniques," below, invest in new technologies. The counterintelligence program should assist in shaping security measures, but leave the responsibility for decisions regarding security to line management; its primary function should be collection, investigation, and analysis. In this respect, the commission recommended that the counterintelligence program strengthen cooperation with the scientific community for information collection purposes; DOE leadership must ensure that counterintelligence officers have access to available information at all laboratories, including the unclassified, open science laboratories. At the same time, the commission recommended removing unproductive security burdens associated with collecting that information, specifically on unclassified foreign scientific collaboration.

The commission also made specific recommendations for clarification or amendment to a number of specific security policies. For example, the commission recommended amending the practices for controlling the confusing area of so-called sensitive unclassified information. The current lack of management discipline around this type of information both hinders the scientific enterprise and reduces the ability of security professionals to control this information where necessary. In the commission's view, if information requires protection, it must be classified or protected by proper administrative controls that are based in statute and have clear definitions for use.

4. Adopt New Tools and Techniques. Fourth, the commission recommended that DOE augment its capabilities for security and counterintelligence with significant investment in new tools and techniques. Specifically, DOE must develop and invest in state-of-the-art technologies for personnel authentication, access control to cyber systems and facilities, and data fusion and analysis techniques. The Department should invest in biometric and other systems that would help make authentication and access control processes more robust and less intrusive. By employing new technologies, DOE could strengthen positive identification of employees and visitors and significantly reduce cumbersome physical and cyber access requirements. In parallel, the commission recommended that DOE invest in databases, information systems, and analytical tools to perform data cross-correlation, data mining, and analysis for security and counterintelligence purposes. Such tools are badly needed in order to strengthen the analytical capacity of the counterintelligence program.

5. Strengthen Cyber Security. Finally, the commission recommended that DOE devote priority attention to strengthening cyber security; it is both the strength and the Achilles heel of the scientific enterprise. Other parts of the commission's report contain recommendations that would improve cyber security, but the commission also made several additional recommendations that are specific to cyber security. First, the role of the Chief Information Officer (CIO) in DOE and NNSA should be strengthened by ensuring that he/she has responsibility for cyber security, so that development of cyber security policies are integrated with information technology systems policy. The commission also recommended that DOE establish a cyber security advisory panel that utilizes the knowledge and experience of outside experts, to bring cutting edge solutions to the DOE cyber enterprise. Finally, the commission underscored that DOE must place a higher priority on timely implementation of cyber security solutions that are already developed, and do more to evaluate emerging technologies being developed by other agencies and the private sector.

Conclusion

When the Department released the commission's report in June 2002, it said that it had implemented, or was in the process of implementing, many of the commission's recommendations, in part as a result of dialogue with the commission as work was underway. It is still early, however, to be able measure any results. The commission has offered its services to assist in any follow-up that the Secretary may request in these implementation efforts. As the commission noted in its report, DOE is at a critical crossroads. The future strength of the national laboratories is imperiled. The commission hopes that the DOE leadership recognizes its options: The Department can continue to muddle through with security and counterintelligence procedures that are out of date and undermine the health of the national laboratories. Or it can seize the opportunity to lead the way in the federal government with development of a modern, risk based security model.

This article was excerpted in large part from "Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department Af Energy Laboratories."
For questions about the Commission on Science and Security, contact Anne Witkowsky, Commission Director, Center for Strategic and International Studies, 202-775-3291 or awitkowsky@csis.org

Anne Witkowsky, Senior Fellow
Technology and Public Policy Program
Center for Strategic and International Studies
1800 K Street, N.W., Washington, D.C. 20006
(202) 775-3291(ph); (202)775-3199 (fax)
awitkowsky@csis.org