

Testimony to the 108th Congress, House of Representatives
Committee of Government Reform
Subcommittee on National Security, Emerging Threats and International Relations
June 24, 2003

Good morning, Mr. Chairman. I would like to thank you and the subcommittee for inviting me to give my professional opinion on the state of security at the nuclear weapon facilities in the Department of Energy. I look forward to presenting to you a serious national security problem that only Congress can solve that has the potential consequence equivalent to 9/11.

For the past 20 years I have been continuously participating in security programs for all of the Class A facilities and transportation of Category I quantities of special nuclear materials in the Department of Energy. I am currently doing more limited work in security at the Department of Energy operations office level that keeps me current in Department of Energy activities. My contracted work consisted of security engineering of detection systems (typically alarms and closed circuit television) and delay systems (typically barriers) and vulnerability analysis of the risk to the nuclear materials from theft or sabotage. After making my concerns about inadequate security to Department of Energy headquarters, and the current administration, my headquarters work was terminated. Today, I am actively involved in homeland security concerns to include such diverse work as the vulnerability analysis for Mount Rushmore and the National Park Service, and engineering for security of dams for the Corps of Engineers.

In 1997 I began an assignment at headquarters to provide quality assurance of the vulnerability analysis for the Safeguards and Security Plans for the 10 Class A Category I special nuclear materials sites and the Transportation Division. The quality assurance effort was initiated by Col. Edward McCallum the Director of the Office of Safeguards and Security Division for Department of Energy. He is now the Director of the Department of Defense's Technical Security Working Group. The quality assurance program was a team effort of 15 to 20 multi-disciplinary professionals. The team consisted of: Department of Energy headquarters staff; RETA Security, Inc. senior personnel; Sandia Laboratory personnel from the computer tactical simulation lab; and U.S. Army Special Forces personnel on assignment for force on force exercises. All four groups integrated their efforts through all phases of the quality assurance process to include the publication of the final reports. One of the first sites reviewed was Rocky Flats. On March 21, 1997 Col McCallum issued a classified letter to the Rocky Flats Operations Office declaring them to be at high risk. Within months, Los Alamos and the Transportation Division were also determined to be at high risk. The quality assurance team continued to review Site Safeguards and Security Plans and Vulnerability Analysis Reports through the fall of 1999 when we were disbanded by Joe Mahaley director of Office of Security for Department of Energy and Toby Johnson now acting director of nuclear safeguards and security for NNSA.

In the spring of 1998, three Department of Energy employees from the headquarters Office of Safeguards and Security and myself were assigned by Marshall Combs of headquarters Department of Energy to provide technical assistance to Peter Stockton, a special assistant for security to Secretary of Energy Bill Richardson. Over the next 18 months, until the fall of 1999, the special assistant and I prepared 13 classified white papers for the Secretary outlining a variety of security risks at the various Department of Energy sites. These papers not only disclosed vulnerabilities, but also disclosed cheating and altering of risk ratings for various sites and the transportation division by Department of Energy management.

The information, documentation, and data disclosing the high risk were passed up the chain of command from the quality assurance team and down the chain of command from Secretary Richardson. Virtually nothing was done to address the high risk even though Departmental Orders require compensatory remedial actions within 24 hours of the disclosure. Since that time we have raised these concerns with Secretary Abraham, and once again, other than denial, nothing was done to address the concerns.

In the committee's letter of invitation sent to me you said the purpose of the hearing was to determine the "adequacy" of security in Department of Energy. The expression "adequate" is a layperson's term. The department has very prescriptive definitions of risk for the consequence of loss of nuclear materials and risk to the health and safety of the public. Risk in a Vulnerability Analysis report is developed as a

quantitative value, that is in turn provided adjectival designations of high, moderate, or low risk. When a site is determined to be at high risk, compensatory measures must be implemented within 24 hours as I mentioned earlier. A simple red flag you should look for in a description of risk is “adequate” which in fact is an obfuscation of a risk state. Based on past Department of Energy policy and management, and my current activities in the department, I fear that we remain at high risk today. I urge you to look into this critical concern. I further urge you not to accept the canned response, “we fixed it” without clear verification. The people who long tolerated and even abetted the failings in the department are still there, with no one else to oversee their actions.

The risk of loss of nuclear materials or the risk to health and safety of the public is from adversary tactics of theft or sabotage. Theft is an action to steal enough nuclear materials to make a nuclear bomb from uranium or plutonium. Sabotage to uranium or plutonium inventories can create either an improvised nuclear device or a radiological dispersal device. The department first recognized the problem of improvised nuclear devices in 1990. I was a technical consultant on the tiger team that determined where on the various sites in Department of Energy the concern of an improvised nuclear device existed. We also recommended corrective actions to address vulnerabilities at the respective sites. Compensatory corrections were made within 24 hours at all of the affected sites. The problems of improvised nuclear device is an ongoing concern with open issues still plaguing the department today. The issue of radiological dispersal devices was not surfaced in the department until 1995 with the issuing of the Presidential Decision Directive 39. PDD-39 was later augmented with PDD 62 and 63 further addressing weapons of mass destruction. The problem of radiological dispersal devices, like improvised nuclear devices is an ongoing concern with open issues still plaguing the department today

You have asked “what has the assessment shown?” The assessments, particularly the quality assurance teams efforts, documented high risk at certain sites. When for example from 1997 to 2000, over 200 classified and unclassified letters and reports were prepared by the quality assurance team, of which I was a principal author, that identified high risk to three major facilities with tons of highly enriched uranium and plutonium holdings. The assessments included theft of special nuclear materials and sabotage resulting in either an improvised nuclear device or radiological dispersal device. I personally briefed the high risk findings to Joe Mahaley and Toby Johnson. Neither one acted in accordance with Department of Energy Orders. Some of these same issues were briefed to Secretary Richardson and he staffed them to the same two persons and nothing was done to address the vulnerabilities. Members of the quality assurance team surmised that what happened in these instances was that OSS (now the Office of Security) would float the issue to the two responsible program offices, Defense Programs and Environmental Management, where there would be immediate reluctance to address the issue. There was continuous “foot dragging” by each of these program offices in regard to evaluating the consequences of loss of nuclear materials or the definitions and characteristics of the design basis threat. For example, when developing a worst case scenario, the quality assurance team would often assume to arm the terrorists with a 50 caliber sniper rifle with armor piercing incendiary rounds - the program offices would argue that this was unfair to the protective forces! Regularly, the program offices would balk at the high risk determination at a site because if they were to acknowledge the state of risk they would have to fix it and institute immediate compensatory measures and that would divert funds from programmatic efforts. Why was there no action? There are a variety of explanations to include:

I.culpability - management would have to acknowledge past problems

II.cost potential - large expenditures to fund operating dollars for increased security forces and facility dollars for hardware

III.politically incorrect - those who subscribe to the problem have disappeared through reassignments.

How is risk assessed? The department uses a standard risk equation developed in the early 70s. The equation for risk (R) is:

$$R = C \times T \times (1 - PE).$$

IV. The term “C” is the value of consequence of loss used for theft or sabotage of nuclear materials and danger to the health and safety of the public.

V. “T” is a value assigned to the design basis threat, such as terrorists

VI. PE is a value for the basic elements of a physical security systems used at the sites in Department of Energy to protect the nuclear assets and consists of detection, delay and response.

In and of itself the equation for risk is algebraically simple, perhaps deceptively so. For example, in physics the equations developed by Newton and Einstein, $F = ma$ and $E = mc^2$, are also simple. However, one determines space flight and one develops nuclear weapons. The risk equation in Department of Energy is used to determine the protection required for assets of societal importance, i.e., theft or sabotage of nuclear materials from the national inventory under the stewardship of the Department of Energy.

It is important to note that when determining risk the protection effectiveness “PE” term is TIME sensitive. Terrorists, whose goal may be theft or sabotage, want to minimize their time to accomplish their objective. For example, a time line tested at a Department of Energy site was 34 seconds to steal 20 Kgs (44 lbs) of high grade uranium! The determinant factor in thwarting a terrorist act is the ability of the site’s protective force to interrupt and neutralize the terrorist. Simply put, can the protective force kill the terrorist before the terrorist is successful? We failed the TIME trial on the USS Cole and at the Dahran barracks just to name a few recent examples of national failures in security when we were on high alert to terrorist acts.

Today, the department has no “KILL” standard. Historically, we have seen guard forces sized and equipped with the “last man standing” criteria. This criteria means we have a guard force with just enough capabilities so that in an engagement between the terrorists and the protective forces the protective force will have one man left after the battle! During the quality assurance effort, we proposed a definition for a robust guard force protecting against theft or sabotage that included such basic elements as: guard force size per shift; tactics of denial, containment, recapture, recovery; and armament. No standard policy exists today for what a margin of prudence is necessary for a protective force to ensure the protection of nuclear materials. If you need more guards to ensure a win with a margin of error, their cost is an overhead operating budget item which will reduce programmatic efforts. If we don’t subscribe to the reality of a terrorist act, minimal dollars will continue to be set aside for protection in the nuclear weapons complex. The existing protective force management in the department does not allow any margin of error.

The continued concern for protection of nuclear materials and the safety of the public resulted in my writing a confidential letter to the “czar” of security for the Department of Energy in January 2000 expressing my concerns and accusing Joe Mahaley and Toby Johnson of lying about the state of security in Department of Energy and the high risk to theft and sabotage of nuclear materials. The “czar” never contacted me about my allegations, but simply turned my letter over to the Inspector General’s Office. After 10 months the IG said it could find nothing to refute the “high risk” determination contained in the 200 unclassified and classified documents given to them. Because the accusation of “lying” could not be proven, the crucial charges were dropped with the contention that management was aware of the high risk. To paraphrase a recent quote from Steve Wallace of the Columbia Accident Investigation Board “what seems to have evolved is that higher-level decision makers came to the conclusion that there *isn’t a security issue* in part based on an analysis done by analysts who sort of wanted *low risk*.¹⁴ In January 2001 I approached the Project On Government Oversight (POGO) and together with Peter Stockton, the special assistant to Secretary Richardson, we co-authored a report “US Nuclear Weapons Complex: Security at Risk.” This report detailed the high risk in the department’s nuclear weapons complex. The report was 99% complete on 9/11/01 when the greatest terrorist act against this nation occurred. The Department of Energy complex was at high risk then against a much simpler terrorist design basis threat than used in the actual attack on 9/11, or that used most recently in the Riyadh compound attack.

¹ Tribune Newspapers, Michael Cabbage, 6/6/03.

Nineteen months after the September 11th attack, a new design basis threat was finally issued on May 28, 2003. A draft version had been circulated on 12/31/02 that included an increase in the number of terrorists **and** a lowering in the numerical value for low risk. The draft design basis threat would have approved one failure in every 20 attacks to be at low risk. Today's new design basis threat approves a considerably higher rate of loss. It is the same rate used before the 9/11 attack. On 9/11 the terrorists succeeded in three out of four attempts. Either an addition to the number of terrorists **or** a decrease in the approved low risk would result in a linear increase in the size of the protective force for a given site. By making just one change to the design basis threat, the security improvements are simplified. Even with the new and simple changes to the design basis threat, the necessary implementation schedule for funding of security improvements are not required to be completed until 2009 with the actual implementation to follow some time later!

The department has been at risk to theft and sabotage since 1997 to a simpler threat that was often "dumbed down" by program offices. For example, please recall the hew and cry about 50 caliber sniper rifles referred to earlier in this testimony. Today, we are at an even greater risk with any increase in the design basis threat whether it is increased numbers of terrorists or the reduction in the value of low risk. The increase in the number of adversaries results in the need for timely response of the protective force with two to three times more personnel for each "new" adversary. If the approved risk is lowered, the same type of increases to the protective force size is also needed. Funding, hiring and training of a larger protective force takes at least 18 months. Livermore Labs disbanded their special response teams in 1995, when it was pointed out to them that they were at high risk in 1997, it took them 18 months to reconstitute the force.

I have talked about the risk to the nuclear weapons complex in the department and the risk to the health and safety of the public as well as the lack of corrective action for a just approved design basis threat, but how do we fix it? There is no quick fix in a department that has been dysfunctional² as long as the Department of Energy has, but there are corrective steps to start the improvement process. The are:

VII. Hold senior managers in the department accountable for their actions. Many of the current managers in the department knew and know about high risk to the nuclear inventory from theft or sabotage and they were given thousands of pages of classified reports documenting the high risk. To date reorganization of the department, to include NNSA, has only rearranged the deck chairs. We need to replace these persons with qualified personnel. The bureaucrats in place protect one another. You can't expect friends to fire one another. In this case only the congress can affect change. Top leaders should be held accountable. Their action should put their careers on the line. Today, one of the aforementioned Department of Energy directors has been given an award and the other is at Lawrence Livermore Laboratory looking into the security failure of the lost security keys! What we need are qualified persons with experience in loss-prevention, not simply retired military persons whose experience is in national defense or law enforcement.

VIII. Consolidate the nuclear materials to central repositories in a timely manner. Secretary Richardson, before he left, signed a Decision Directive to move nuclear materials from Los Alamos. It is still being planned three years later with the movement of nuclear materials on a distant horizon. This is an example of malicious compliance by current departmental managers and program offices.

IX. Provide line item funding for physical security at the level of a program offices to include operating dollars designated for increased protective forces size and capabilities. Today the Department of Homeland Security has a budget greater than \$30B. However, Department of Energy management resists spending money on security. If they establish a new 24/7 post or patrol for the protective force at any of the Class A sites, this is equal to about five full time protective force personnel which is the same cost as two or three scientists. Therefore the scientist

²Special Investigative Panel of the President's Foreign Intelligence Advisory Board. June 1999.

must be laid off to hire the security personnel - not a popular option. The program offices have an inherent conflict of interest when deciding to improve security and lower risk or lay off scientists.

This panel has diverse backgrounds, professional training, and expertise, but we have arrived at the inescapable conclusion that the Department of Energy weapons complex is at risk.

POGO has gathered and assimilated a lot of information from informants and whistle blowers that has been thoroughly examined and summarized to determine the status of security in the Department of Energy complex to include not only concerns about theft and sabotage to nuclear materials, but also espionage and fraud.

My corporation, along with other professionals from Department of Energy, Sandia and the Army's special forces have exhaustively documented departmental vulnerabilities during the quality assurance effort. They have provided practical input to worst case scenario development and they have tested and stressed protective forces in the complex with force on force testing. They have helped address weaknesses in: tactics, armament, and size of the protective forces. Through the use of surprise, violence of action, and fast time-lines they can fully exploit vulnerabilities and then prescribe actions to correct the weaknesses and vulnerabilities.

The information presented by this panel to you was developed from diverse sources which agree that Department of Energy is doing too little too late to address the risk in the complex.

In conclusion, let me summarize my testimony. Many of the nuclear weapons facilities in the Department of Energy are at risk which endangers the health and safety of the public. This has been documented continuously since March 1997. The security for the nation's nuclear stockpile has been mis-characterized as "adequate" by career senior personnel within the department. The corrections and remedies for the existing problems falls to Congress for action.

Ronald E. Timm, Certified Protection Professional
President
RETA Security, Inc.