Testimony of Richard Levernier

House Government Reform Subcommittee

National Security, Emerging Threats, and International Relations

February 14, 2006

Mr. Chairman:

Thank you for holding this hearing to consider whether current whistleblower legal rights sufficiently protect national security employees against retaliation. My name is Richard Levernier. I have dedicated my entire career to public service: in the United States military, as a metropolitan and federal law enforcement officer, and for more than twenty-three years as a nuclear security specialist for the U.S. Department of Energy (DOE). I retired effective January 3, 2006.

Until August 2000, I was the DOE Quality Assurance (QA) Program Manager for Nuclear Security. My job was to manage a team of experts that reviewed the security plans for DOE nuclear weapons' sites, and to conduct performance tests to confirm risk determinations and identify vulnerabilities before they became major national security threats. Our QA team oversaw security effectiveness for the entire nuclear weapon's complex, from research and development at the national laboratories to bomb manufacturing to the storage of Special Nuclear Material to the transportation of nuclear weapons. I utilized a team of world class experts to evaluate each security plan. Our expertise included systems engineering, vulnerability assessments, computer modeling, physical security systems, nuclear material safeguards, protective forces, performance testing, special weapons and tactics, and military special operations, including active duty U.S. Army Special Forces.

Among my responsibilities was to devise "adversary" tactics and perform command and control operations during force-on-force tests at nuclear weapons facilities. These tests pit an outside expert adversary force, "mock terrorists," against the site protective force using specially modified laser-equipped weapons to enact an actual armed engagement. Despite artificial limits placed on our ability to surprise defenders and obligations, such as obeying government-posted speed limits, stop signs and OSHA regulations, the "terrorists" I commanded would win force-on-force tests more than 50

percent of the time, year after year. These results were extremely troubling, considering that actual terrorists – who would *not* be obligated to coordinate their attack schedule with the security forces or to observe speed limits and avoid building ladders and climbing on roofs – would likely overwhelm site protective forces. Moreover, even the so-called "wins" were suspect. In tests in which the protective forces "prevailed," security forces were often suffering 50 percent or greater casualties or indiscriminately "slaughtering" crowds of evacuating employees. Yet, all that was recorded after these tests was a "win" for the contractor protective force.

This subcommittee has heard detailed testimony in the past on the specific shortcomings of force-on-force testing, as well as systematic security deficiencies throughout DOE. My testimony is relevant today, because I am a direct casualty of the DOE culture that refuses to take the corrective actions necessary to responsibly address these problems that continue to endanger U.S. national and homeland security.

Five years ago, DOE management effectively ended my career as a nuclear security professional by removing my security clearance and transferring me to unclassified duties. In retaliation for sending an unclassified Inspector General report to the media, DOE made an example out of me to all other would-be whistleblowers; I was stripped of my QA security responsibilities and transferred to a windowless basement storage room in the DOE Germantown building, where my primary job responsibility for three years was to manage DOE's official foreign travel program, an administrative function completely unrelated to national security.

The agency's primary stated rationale for taking these actions was that I had made an "unauthorized dissemination of sensitive government information." The U.S. Office of Special Counsel determined that the retaliatory actions taken by DOE were illegal under the Whistleblower Protection Act (WPA) and the anti-gag statute. However, the WPA could only lead to token help – rescinding a two-week suspension. My career as a nuclear security professional could not be restored because I had no way to challenge the suspension of my security clearance, which was unlawfully taken in retaliation for the exact same protected disclosure.

I am testifying today for the same reason that I first disclosed evidence of nuclear security breakdowns at DOE: based on my extensive experience protecting U.S. nuclear

facilities, material, and weapons, I believe that critical deficiencies at the heart of the Department of Energy's safeguards and security program place the health and safety of the American public in grave jeopardy. Unfortunately, my concern for the national security of this country and my impatience with the reluctance of the Department to make vital security reforms placed me on a collision course with senior management at DOE. DOE is fully aware that many of the security problems I identified as a whistleblower four years ago persist and has not taken actions to correct them. Given the significant increases in the terrorist threat which has been universally acknowledged since 9/11, the degradation of national security that results from these deficiencies is now greater than ever. Moreover, the chilling effect of DOE's unlawful retaliatory actions taken against me has been an effective deterrent to others who consider blowing the whistle. I am hopeful that sharing my experiences with Congress will help move this body to strengthen the protections for individuals blowing the whistle on sensitive security issues and, in turn, help to create an environment in which vulnerabilities are addressed in a timely manner, consistent with our nation's security.

I. DOE Service

I had a flawless, exemplary record at DOE until I began internally blowing the whistle on safeguards and security breakdowns in 1997. My DOE service began in the Chicago Operations Office in 1979, where I served as a personnel and physical security specialist. After several promotions and subsequent assignments at the Savannah River Operations Office and at DOE HQ, from 1990 to 1995, I served as the Director of Safeguards and Security at the DOE Rocky Flats Office in Golden, CO. I managed a staff of 50 federal and support contractor security professionals at a facility with an annual safeguards and security budget of more than $50 million. While at Rocky Flats, I was responsible for management and oversight of a contractor protective force with more than 500 armed personnel at a nuclear weapons production facility with 9,000 employees. Rocky Flats maintained an inventory of more than 13 metric tons of Special Nuclear Material (SNM), enough material to fabricate hundreds of nuclear weapons.

In March 1995, I returned to DOE HQ, Germantown, MD, and shortly thereafter started my work as the QA Program Manager for nuclear security. Over the years I was

responsible for the identification and reporting of dozens of serious national security vulnerabilities at DOE facilities. These vulnerabilities and the associated documentation were usually classified due to their national security significance.

I was fully dedicated to ensuring our country's national security for the public health and safety of our citizens. However, due to a multitude of factors, DOE management became increasingly resistant to addressing confirmed security concerns. In turn, I became increasingly frustrated with my inability to effectively communicate serious security vulnerabilities to my management and facilitate the corrective actions necessary to address the problems. These serious vulnerabilities were not my personal opinions. Rather, they represented the consensus conclusions of the DOE security plan QA team. They were corroborated by a litany of internal and independent security reviews, ranging from congressionally chartered commissions to GAO analyses to numerous DOE Inspector General Reports, as well as non-governmental findings and most recently a comprehensive independent DOE/NNSA security review made public in September 2005.

II. Internal Whistleblowing at DOE

1. Resistance to Addressing "High Risk" Quality Assessment Review at Rocky Flats

In March 1997 the QA review team I managed concluded that the Rocky Flats site was at "High Risk," an unacceptable condition in DOE. The geographic location of Rocky Flats, coupled with the types of DOE assets located there and the nature of the security vulnerabilities constituted a serious and substantial threat to the people of Denver, CO and surrounding areas. The High Risk conditions were largely the result of an inadequate protective force capability to respond to a terrorist attack. Because Rocky Flats has been de-inventoried and the issues are no longer exploitable, they're no longer classified. The QA team found that protective force response ability was inadequate for a number of reasons, including (but not limited to) --

- an insufficient numbers of responders;
- responders not properly trained and equipped to address the threat, i.e. a lack of long range weapons. If an attack came from the surrounding mountains, terrorists

would have the ability to shoot down at defenders, but defenders would be helpless and could not fire back at such a long-range.
- similar to what we are currently seeing in Iraq, a lack of hardened response vehicles, such as armored humvees, created an exploitable vulnerability.
- radio communications susceptible to simple jamming.
- alarms that failed to distinguish between tamper, intrusion, and line supervision;
- unacceptably high false alarm rates, causing hundreds of unnecessary protective force responses and complacency by the protective force and plant employees.

I repeatedly documented my team's concerns, through a succession of classified memoranda, to my supervisor. I was repeatedly told that I was creating unnecessary problems, and to "Back off." In an effort to work within the constraints of the system, I began forwarding all my QA reports to my second level supervisor. While my second level supervisor fully supported and was receptive to QA inputs, the program continued to experience bureaucratic resistance from my immediate supervisor. This resistance took the form of QA exclusion from key meetings, arbitrary resource reductions, and decisions to limit the QA scope without appropriate justification. About the end of 1998, my second level supervisor was removed from his position for his outspoken and critical views concerning the status of Safeguards and Security in DOE.

2. Resistance to Implementing Recommendations in President's Foreign Intelligence Advisory Board DOE Security Review

About this same time, numerous high visibility security problems surfaced, including many at Los Alamos National Laboratory (LANL), and external reports critical of DOE's management of Safeguards and Security. Primary among these was a report issued in June 1999 by the President's Foreign Intelligence Advisory Board (PFIAB), "Science at its Best / Security at its Worst, A Report on the Security Problems at the U.S. Department of Energy." (http://www.fas.org/sgp/library/pfiab/) The PFIAB Report contained dozens of significant findings and recommendations which I believe were largely ignored by DOE. The PFIAB report documented these alarming DOE security mismanagement trends:

> **"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...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...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, 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."

The PFIAB findings and recommendations covered the entire spectrum of safeguards and security activities, including – security and counterintelligence accountability; external relations; personnel security; physical/technical/cyber security; and business issues. DOE's failure to address these significant issues, consistent with established policy, contributed to overall inefficiency of the safeguards and security program and seriously degraded U.S. national security.

Shortly after the report was issued, I initiated actions to ensure that the PFIAB findings and recommendations were implemented into the security plans. When my (new) immediate supervisor became aware of my initiatives, I was directed to stop. When I reminded my supervisor of the pertinent requirement in the report (and in DOE

policy) to *track and address* safeguards and security deficiencies and findings I literally was told to, "Forget about the PFIAB Report."

3. Addressing Vulnerabilities at Rocky Flats and Transportation Security Division through New "Security Czar"

Despite internal DOE reluctance to implement the report's recommendations, findings such as those in the PFIAB Report and the related security scandals convinced DOE Secretary Bill Richardson to create a position of "Security Czar." Retired U.S. Air Force General (four star) Eugene Habiger was selected to fill this new role. Around the time of General Habiger's appointment, the QA program identified unmitigated "High Risk" conditions in the Transportation Safeguards Division (TSD) and Los Alamos National Laboratory's security plan. Additionally, the vulnerabilities identified several years earlier at Rocky Flats remained unresolved.

The lack of an approved security plan at Rocky Flats was becoming a more visible administrative issue and ultimately came to the attention of the new Security Czar. General Habiger selected me to lead a team of my choice to Rocky Flats, to provide all necessary assistance and to resolve outstanding security concerns. Additionally, HQ concurrence authority was delegated to me by General Habiger, specifically for the Rocky Flats security plan. My superiors were very unhappy with General Habiger's direct tasking of this high profile assignment to me.

On October 1, 1999, I briefed my immediate supervisor on the plans for the Rocky Flats security plan assignment. My recommended actions to remedy this situation included:

1. obtaining longer range weapons for selected responders;
2. reassigning numerous vulnerable responders to posts inside protected buildings;
3. consolidating nuclear materials into fewer vaults/targets to increase the numerical superiority of the protective force responders;
4. developing response plans and procedures that were less dependent on effective radio communication that was susceptible to jamming;
5. increasing protective force training while reducing the tactical complexity of the response plans and procedures;
6. improving the reliability and speed of essential electronic alarm systems;
7. improving the testing and maintenance of all critical security systems.

During this briefing session, my supervisor stated that I had circumvented the chain of command, failed to keep him fully informed, and threatened me by stating, "[Your] actions had been duly noted and there would be consequences." In spite of this hostility, due to General Habiger's support I successfully implemented my recommendations at Rocky Flats. In recognition of this accomplishment, I received a $5000.00 performance award.

The vulnerabilities identified by QA review of the Transportation Safeguards Division security plan were extremely serious and posed a significant risk to national security. TSD is responsible for transporting DOE assets, including nuclear weapons, in specially equipped trucks by convoy throughout the United States. The specific exploitable vulnerabilities are classified and cannot be discussed.

In addition to issuing a succession of classified memoranda describing the results of our TSP security review, the QA team briefed my chain of command in detail. Despite my best efforts to convey the seriousness of the TSD vulnerabilities, no action was taken for more than six months! Finally, as a last resort, on November 4, 1999, I prepared a package of the pertinent classified documents highlighting the vulnerabilities at TSD, and transmitted them, by appropriate means, to Mr. David Jones, General Habiger's Executive Officer. General Habiger was immediately made aware and appropriate compensatory and longer term corrective actions were taken. My supervisor later told me he suspected me of, "jumping the chain of command again," and that, "I would pay for it." A month later, in December 1999, I received a lower annual performance appraisal than prior ratings. My supervisor told me the reason for the reduced rating was because I was not considered a team player by management.

4. Participation in DOE OIG Investigation

On January 5, 2000, the president of a security engineering consulting firm for the QA Program I managed wrote a letter to General Habiger that described lying in reports on the security status at nuclear sites and retaliation against individuals trying to correct the security problems. General Habiger forwarded the letter to the DOE Office of the Inspector General (OIG), which resulted in a high profile and lengthy investigation of the allegations.

The OIG Inspection Report, "Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process (SSSP)," found "[s]ubstantial differences in what was being reported as the actual status of security at Department sites by the SSSP QA function, and what was being reported by the cognizant sites." DOE management was well aware that I was interviewed by OIG representatives on multiple occasions, including one trip to Albuquerque, NM specifically to meet with OIG inspectors. I estimate that I was interviewed by OIG representatives for approximately 25-30 hours over 6-8 weeks. Since the complainant and his principal staff engineer worked directly for me supporting the QA Program, and had done so for many years, we (QA) were viewed by management as "collaborators," and I was held responsible.

On many occasions my superiors told me that my zeal for finding problems was not appreciated and my career would suffer as a result. I was also told on many occasions that I was "responsible" for my support contractors, and that they needed to be "muzzled." Additionally, upon learning of the letter from the contractor to General Habiger, my immediate supervisor told me that the complainant would not work for DOE much longer after making these types of formal accusations against management. Not surprisingly, not long after the OIG report was issued, the contractor was completely eliminated from DOE work.

III. Looking for Relief outside DOE

In 1999, I was assigned to provide technical support to a Special Assistant to the Secretary of Energy, Mr. Peter Stockton, who was evaluating a wide range of security related issues and problems at Los Alamos National Laboratory (LANL) and in the Transportation Security Division (TSD). While evaluating cheating during force-on-force exercises at LANL and TSD, numerous serious irregularities in the DOE Albuquerque[1] security plan program were brought to our attention. While Mr. Stockton was very concerned with the survey program allegations, he referred the complainant to the OIG. The executive summary of the resulting OIG report stated:

[1] Prior to the establishment of the National Nuclear Security Administration (NNSA) in 2000, regional DOE field offices were responsible for security oversight of the national laboratories. The DOE field office in Albuquerque oversaw these responsibilities at Los Alamos National Laboratory and Sandia.

1. Albuquerque management changed [security] ratings for the 1998 and 1999 surveys without providing a documented rationale for the changes.[2]
2. Albuquerque management did not fully address concerns about a compromise of force-on-force exercise during the 1998 Albuquerque Security Survey at LANL.
3. The 1997 and 1998 Albuquerque Security Survey work papers were destroyed contrary to Albuquerque policy on the destruction of records.

The OIG also found:

1. Approximately 30 percent of the LANL Security Operations Division personnel interviewed, who had been involved in the conduct of self-assessments, believed they had been pressured to change or "mitigate" security self-assessments.
2. Some security self-assessments required by LANL were not being conducted.
3. DOE's Los Alamos Area Office security staff was not performing all of the oversight responsibilities associated with the LANL Security Operations Division programs.

When my supervisor gave me a draft copy of the OIG Report in April 2000, I was told it had been officially determined to be unclassified and non-sensitive. The report was reviewed by the DOE Office of Nuclear and National Security Information, Document Declassification Division, which is DOE's ultimate authority on classification matters. Their written determination was issued on March 29, 2000, and stated:

> "**We have determined the documents are unclassified, accordingly, we have no objection to their release to the public.** You are reminded that bibliographical information from all declassified and publicly releasable documents must be made available for inclusion in OpenNet. We are providing the procedures for furnishing OpenNet with the required information."

As an experienced security professional, familiar with the DOE security survey program and the complex long-standing security issues at LANL, I was shocked by the OIG findings. LANL is a major DOE facility, with multiple attractive targets from a threat perspective. The security survey program is DOE's only comprehensive oversight mechanism. The OIG inspection report conclusions were incredible: the survey program was unsound, ratings were being manipulated, documentation was being destroyed in a

---

[2] DOE Order 470.1 mandates a "Safeguards and Security Program." The purpose of the Order is to ensure appropriate levels of security protection consistent with DOE standards to prevent unacceptable, adverse impact to the national security. The Order establishes that the responsible Operations Office (in this case, Albuquerque) assign ratings of "unsatisfactory," "marginal," or "satisfactory" based on conditions existing at the end of security survey activities; and that survey reports include a justification and rationale for the overall composite facility rating.

cover up, and self-assessment team technical experts were "being pressured" to minimize the reporting of problems to make LANL "look good." My overall assessment of the OIG findings was that security problems at LANL were being intentionally disregarded, inaccurately reported and inappropriately factored into ratings that ultimately are reported to the President.

Given the devastating consequences of the loss of control of DOE assets, including the possibility of an unauthorized detonation of a nuclear weapon on U.S. soil, I was gravely concerned about the implications of the OIG report and the overall degradation of security conditions at Los Alamos – and throughout DOE. Based on my previous experiences, I was also concerned that the OIG report would simply gather dust within the growing collection of reports critical of DOE security and be overlooked by management without taking the necessary actions to address the problems. Given these factors, I believed that it was my duty to provide the UNCLASSIFIED and non-sensitive report to the public, and the only way I knew how to do this was through the media. I believed that providing this public information to the press would serve as a catalyst for improvement in one of DOE's core Security Program elements and thereby enhance our National Security.

On June 26, 2000, I sent to the media a copy of the unclassified draft OIG report that had been provided to me by my supervisor with the previously-noted markings, i.e. "we have no objection to...release to the public." The final version with essentially the same information that *already* had been published on the DOE OIG web site in May 2000, prior to my forwarding it to the media. Because I was afraid of retaliation from DOE for getting the media to focus on these critical and potentially embarrassing issues, I used another DOE employee's name on the facsimile cover sheet when I transmitted the information to two newspapers. Only one of my attempted transmissions was successful; the second failed due to technical reasons and ultimately led to a DOE investigation of the release.

IV. Fallout

The content of the draft IG Report I disclosed to the media was very embarrassing to DOE and numerous senior officials in my chain of command, so DOE opened a

criminal investigation to find out who did it. DOE issued a Letter of Authority to conduct an investigation on July 18, 2000, which stated, "This letter authorizes and informs all concerned parties that the Office of Security Affairs has initiated a formal Preliminary Investigation into potential criminal violations of Title 18 and 42, United States Code, concerning a potential unauthorized disclosure of sensitive and/or classified national security information transmitted via unclassified facsimile to a Washington DC newspaper editor."

During the investigation, which was conducted in early August 2000, I readily admitted that I sent the report to the media. In an effort to address what I thought was the relevant and central issue, **I told investigators that no sensitive or classified information was involved** and volunteered to take a polygraph test to confirm the accuracy of my statements. I understood and acknowledged that using a different name on the facsimile cover sheet was very poor judgment on my part and wanted to set the record straight and ensure that there were no consequences for the other person. I also told investigators that my motivation was to have media coverage serve as a catalyst for improvement of the DOE security program.

On August 17, 2000, I received a letter from the Acting Director of the DOE Office of Safeguards and Security informing me that my security clearance had been suspended effective immediately. The letter stated, "**This action is based on your unauthorized dissemination of sensitive government information to The Washington Post and USA Today**..."

On October 26, 2000, I received an official "Notification Letter" from the new Director of the DOE Office of Safeguards and Security along with a "Summary of Information Creating a Substantial Doubt Regarding Continued Eligibility for Access Authorization." The summary cited two additional documents which were used to support DOE's decision to suspend my security clearance: 1) a March 18, 1999, memorandum from the Director, Office of Security Affairs, to all Federal and contractor employees in the Office of Security Affairs and Office of Safeguards and Security, restricting the release of classified and sensitive information, and 2) a "Security

Responsibility Statement" that was attached to the memorandum, which I signed on March 29, 1999.[3]

The author of the March 18, 1999 memorandum directly and indirectly led the security clearance actions taken against me. This person, as the Director of the Office of Security Affairs was the security official most responsible for the misconduct covered by the OIG report. He had every motive to feel highly threatened by my disclosures, since they raised issues for which realistically the buck could stop with him.

The October 26 "Notification Letter" also informed me of my options in challenging the security clearance action taken against me. Had I chosen to appeal my security clearance suspension within DOE, this same Office of Security Director (despite his conflict of interest and lack of impartiality as the individual that directed the suspension) would have served as the ultimate appeal authority and "Deciding Official" on the suspension. Stated simply, **DOE "due process" on security clearance actions afforded me the opportunity to ask the individual threatened by my whistleblowing and responsible for initiating the retaliation to change his mind.** I was told that I could attempt to keep my security position by appealing the clearance suspension, but if I exercised this so-called "appeal" and lost, I would be fired. I elected not to appeal and lose my job outright, and instead accepted reassignment to a job not requiring a clearance, at which point the review of my eligibility for a security clearance was terminated. DOE has maintained since 2000 that I "voluntarily transferred" to my new position in the Office of Foreign Visits. However, my decision not to challenge the reassignment was coerced and not voluntary.

In addition to the security clearance action taken against me, informally I was being advised that DOE was considering firing me, whether or not I appealed the security clearance decision. Although I believed the facts in this case clearly did not warrant removal, I was understandably alarmed that such an action was even being considered.

---

[3] Although these forms were cited by DOE in suspending my clearance, they were illegal gag orders according to the terms of the anti-gag statute. Since 1988, Congress has passed an appropriations rider commonly referred to as the "anti-gag" statute. The statute bans spending by agencies to implement or enforce nondisclosure (gag) orders that do not specify that an employee's rights to disclose waste, fraud, abuse, or illegality and to communicate with Congress supersede the speech restrictions in the nondisclosure agreement. The current version can be found in Section 620 of the Consolidated Appropriations Act of 2005 (P.L. 108-447).

Meanwhile, in an effort to further retaliate for my disclosure and to chill future dissent, senior DOE managers unlawfully were making an example of me throughout relevant DOE offices in blatant violation of the Privacy Act and DOE policy. The letter suspending my access authorization, dated August 17, 2000, stated, "This letter has been marked "Official Use Only" to maintain the privacy of this matter between you and the United States Government." The letter also said that while my supervisor had been informed that my clearance was suspended, he had not been informed of the reason for that action. DOE Personnel Security Files (PSF) are required to be protected in the same fashion as classified information.

Despite this, I was informed by numerous staff members and coworkers that they were told by my second-level supervisor in open staff meetings, shortly after my reassignment to unclassified duties, that I was responsible for "a serious unauthorized disclosure of sensitive information to the press." Additionally, a professional colleague located outside the Washington, D.C. metropolitan area, told me that my second level supervisor telephoned him specifically to tell him that my clearance had been suspended for "a serious unauthorized disclosure of information to the press." The colleague asked my supervisor if the information was classified and the response was something to the effect, "that was still to be determined." Given the fact that the Report had been officially evaluated as UNCLASSIFIED almost five months earlier, this statement was false. This supervisor had handled DOE personnel security matters and PSF's for more than a decade and clearly was aware of the governing statutes and pertinent DOE policy. He knew the adverse impact his disclosures would cause. These blatant, unlawful smears directly resulted in irremediable damage to my reputation by creating an unwarranted perception that I was untrustworthy as a security professional.

I finally received a "Proposed Notice of Suspension" on February 28, 2001, more than eight months after forwarding the OIG Report. The primary stated basis in the "Proposed Notice of Suspension" for taking disciplinary action against me was that I made an unauthorized release of sensitive information, in violation of the signed "Security Responsibility Statement." (attachment 1)

On April 18, 2001, the Director of the Office of Security Affairs upheld the suspension in a memorandum issued to me, "Notice of Decision on Proposed

Suspension." The letter informed me that I was to be "suspended for fourteen (14) calendar days from your position of Security Specialist, GS-0080-15, for **insubordination as demonstrated by your unauthorized release of sensitive documents.**"[4] I served a suspension from April 22 to May 5, 2001.

DOE's own actions confirm the surreal irrationality of its stated excuse for yanking my clearance. On March 2, 2001, in response to my Privacy Act Request of October 31, 2000, **DOE provided to me the exact same *draft* OIG Report in question for "use of these documents as you deem appropriate."** It is simply ludicrous that DOE suspended my security clearance – effectively ending my career as a security professional – for disseminating to the media a draft OIG report considered to be "sensitive" and then only four months later DOE provided the identical draft OIG report to me without any restrictions.

V. The Office of Special Counsel – Unable to Enforce its Findings, Impotent on Issues that Matter

1. OSC Whistleblower Reprisal Complaint

After DOE provided its final decision on my suspension, I filed a whistleblower reprisal complaint on September 26, 2001, with the U.S. Office of Special Counsel (OSC). The OSC investigation of my whistleblower reprisal complaint determined:

1. The March 19, 1999 "Integrity of Security Operations" memorandum and attached "Security Responsibility Statement" constituted an illegal gag order;
2. DOE's imposition of a 14 day suspension without pay was determined to be excessive and retaliatory in nature.
3. My disclosure of the unclassified draft OIG Report was lawful and consequently, a protected disclosure under the Whistleblower Protection Act.

Although OSC's jurisdiction was limited and did not include the DOE security clearance apparatus, its findings are clearly relevant. **The fact pattern used by DOE as the basis for my security clearance suspension and two week employment suspension without pay were identical**. Accordingly, OSC's findings should have been

[4] DOE never disputed the two points that were critical to my disclosure of the OIG report. First, the information was not classified. Second, DOE never alleged that my motive for releasing the report was anything but constructive. The April 18 letter upholding my suspension stated, "While the concern you expressed for the well-being of the public is commendable, the information contained in the report was going to be published upon finalization, and, therefore, released in an authorized manner."

fully considered in the adjudication of my eligibility for a security clearance, but to my knowledge, they were not. OSC determined that the "Security Responsibility Statement" and "Integrity of Security Operations" memorandum were illegal gag orders. Accordingly, using these documents as the basis for information deemed to be "derogatory" in the adjudication of my eligibility for a DOE security clearance (as DOE informed me they were) was inappropriate and unlawful, as was the retaliatory investigation used to "catch" me blowing the whistle.

After removing the illegal gag orders from consideration, the only remaining factor – the use of another employee's name on the fax cover sheet – would be grossly discriminatory as a justification for removing my clearance and ending my DOE security career. Personnel holding security clearances routinely make far more serious mistakes, including criminal violations. I worked in the DOE Personnel Security Program for more than five years and know that the suspension of my security clearance was inappropriate and not consistent with established precedents. DOE personnel holding security clearances engage in extramarital affairs, fail to pay child support and alimony, report arrests for Driving Under the Influence (DUI), reckless driving, and theft (shoplifting) almost daily. I am aware of a specific situation where an individual holding a DOE security clearance hit and killed a pedestrian while DUI, retained a security clearance, was again arrested for DUI and had the security clearance reinstated in less than 18 months. In a directly relevant case, a current DOE senior executive security manager knowingly falsified his Personnel Security Questionnaire concerning his educational level and continues to hold a security clearance. Additionally, hundreds of DOE and contractor personnel have been granted security clearances after admitting numerous instances of illegal drug usage, including minor drug trafficking, signed "Drug Certifications" where they promise to refrain from illegal activity in the future have been granted security clearances. Finally, DOE has granted security clearances to convicted felons who have paid their debt to society, including lengthy prison terms and periods of parole.

In addition, my admittedly improper conduct was acknowledged by DOE to be an isolated incident by a long term employee (28 years of service) with an otherwise unblemished disciplinary record and consistent outstanding annual performance ratings.

The relevant CFR (10 CFR 710.7) states, "The decision as to access authorization is a comprehensive, common sense judgment, made after consideration of all relevant information, favorable and unfavorable, as to whether the granting or continuation of access authorization will not endanger the common defense and security and is clearly consistent with the national interest." DOE's suspension of my security clearance was not in accordance with the stated requirements.

Given all of these considerations, *retaliation* for blowing the whistle is the only possible rationale for DOE's decision to uphold the suspension of my security clearance for over five years. Indeed, that was the stated basis for the action. Unfortunately, the OSC had no authority to challenge this unlawful action.

2. Settlement with DOE

My whistleblower reprisal complaint to the OSC was resolved through a formal Settlement Agreement between DOE and myself in October 2003. DOE required that the terms and conditions of this agreement be subject to a nondisclosure clause. In my opinion, the sole purpose of the nondisclosure clause was to protect DOE from embarrassment and hide the fact that they unlawfully retaliated against me. The terms of the nondisclosure agreement expired on January 3, 2006, when I ended my DOE service. The terms of the agreement were as follows:

- I accepted a one day suspension – an appropriate remedy for using a co-worker's name on the fax sheet I sent to the media. The one-day suspension was not based on the disclosure of an agency document to the media.

- DOE demanded that I withdraw my OSC reprisal complaint and waive the right to file any additional claims based on DOE's retaliatory actions. This did not prohibit my right to challenge or appeal DOE's action on my security clearance.

- DOE included a provision that OSC not seek disciplinary action against any DOE employee for engaging in retaliatory actions against me.

- DOE was required to rescind the 14-day suspension, compensate me for lost pay plus interest, and restore all related benefits resulting from the rescission of the 14-day suspension, including accrual of annual and sick leave.

- DOE was required to expunge and destroy all documentary evidence, files, correspondence, memoranda, etc., related to my 14-day suspension based on the disclosure of the IG Report.

- DOE was required to recognize and acknowledge the requirements of the Anti-Gag statute (P-L 106-554, Sec. 622) and review the two illegal gag orders, memorandum on the subject of "Integrity of Security Operations" and the "Security Responsibility Statement" issued by the Director of the Office of Security on March 18, 1999, and any other subsequent gag orders enacted in the Office of Security.

- DOE was required to pay attorney's fees to my lawyers at the Government Accountablity Project within 30 days of the full execution of the Agreement.

- DOE was required to schedule a training entitled "Guide to Rights and Remedies of Federal Employees Under 5 U.S.C., Chapters 12 & 23, and the Whistleblower Protection Act" for supervisors in the Agency's Office of Security, Human Resources and the Inspector General, who were involved in retaliating against me.

While these terms were favorable, the OSC, under existing laws, was unable to enforce its findings of excessive retaliation on the only issue that mattered for my career – restoring my security clearance. In the end, OSC's positive intervention was limited to DOE admitting it was wrong and returning two weeks pay.

3. OSC Whistleblower Disclosure

While my two-week suspension was rescinded, the deficiencies in DOE's safeguards and security program were not. On January 15, 2002, I submitted a formal written whistleblower disclosure to OSC, which included the specific information provided to the media that served as the basis for DOE's suspension of my security clearance and two week employment suspension. On October 25, 2002, the OSC determined there was a "substantial likelihood" that the information contained in my disclosure constituted a substantial and specific danger to public health and safety. Significantly, this also means that my disclosure to the media was protected free speech under the Whistleblower Protection Act.

My whistleblower disclosure to OSC was 36 pages in length with 22 supporting attachments, alleging that DOE's active and passive misconduct represents gross mismanagement, gross waste, abuse of authority, and sustains a substantial and specific

danger to public health and safety. Some illustrations of the security deficiencies at DOE I challenged include:

- plans to fight terrorists attacking nuclear facilities that were limited to catching them on the way out, with no contingency for suicide squads that might not be planning to leave a facility they came to blow up;

- a policy that posted guards so far away from danger zones (and their weapons) that terrorists would have time to enter and leave – with nuclear bomb material – before even the fastest security forces would have time to respond;

- facilities that in some cases are not even as well protected as an ordinary ATM machine with video surveillance, meaning that protective forces would have to creep along walls and peer around corners while defending nuclear weapons facilities, like in 1930's spy movies;

- security inspectors with inadequate qualifications and therefore limited ability to detect security defects, such as gun ports in hardened guard towers installed backwards and left that way for years (this defect could essentially funnel terrorist bullets into the guard tower); and

- more generally, the passive resistance to change and loyalty to entrenched bureaucratic ruts at DOE that continue to endanger the country despite an overwhelming number of reviews urging security reforms.

The bottom line for my disclosures, which remains relevant today, is that DOE's security culture has left U.S. nuclear facilities with unacceptable levels of vulnerability to potential terrorist attack or sabotage.

OSC ordered the Secretary of Energy to investigate pursuant to 5 USC 1213 (c) (1). The DOE requested, and OSC approved, numerous extensions to the statutory 60 day deadline for DOE to investigate the disclosures. Finally, the Secretary of Energy provided the required report of investigation to OSC on May 29, 2003, more than 5 months beyond the initial deadline.

The report came in just as the Special Counsel who ordered it, Elaine Kaplan, was finishing her term. While not the topic of today's hearing, it is impossible not to note that in my experience the Office's performance disintegrated sharply as soon as she departed. To illustrate, I was not informed of the report's existence until July, even though the statute requires me to respond to the report within 15 days. I was not given the opportunity to see and respond to the report until December 2, 2003, more than six

months after DOE submitted it, and almost two years after initially filing a disclosure that identified numerous vulnerabilities and threats to U.S. national security.[5]

The 25-page DOE rebuttal states that nothing is wrong, that the allegations contained in my whistleblower disclosure are completely unfounded and that there is no substantial and specific danger to the public health and safety. The premise for this conclusion is that DOE policies are the baseline for an effective security system. The authors somehow then conclude that since my allegations describe contrary practices, I must be wrong. That begs the question. The point of my disclosure is that the paper policies are being systematically violated in the field.

The DOE report states that my disclosure contains outdated information and that numerous improvements have been made since my disclosure. In support, DOE accepted at face value reassurances from its Office of Independent Oversight, which compiled the report. But there is no basis beyond blind faith to accept those conclusions. The Office of Independent Oversight failed to offer any evidence to support the innocent verdict it gave itself, failed to interview the supporting witnesses I identified, and failed to disclose the methodology used to support its determinations, in violation of statutory requirements (5 USC Sec. 1213(d)).

Of course, some of the information in my whistleblower disclosure is dated and DOE has made some security changes that are unknown to me, because my security clearance was removed. This committee, however, does not have to accept my word as a basis for concluding that the majority of DOE's conclusions in its response to my disclosures are simply a whitewash of longstanding security deficiencies at DOE nuclear facilities. In the two and a half years since DOE concluded that all of my whistleblower disclosures were dated or unfounded, no less than a *dozen* subsequent, relevant reports, including GAO testimony before this subcommittee, have specifically corroborated many of the issues I raised in my January 2002 whistleblower disclosure. These include:

1. MAY 2003: GAO Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, "NUCLEAR SECURITY: NNSA Needs to Better Manage Its Safeguards and Security Program," GAO-03-471;

[5] It should be noted that there is no legal rationale for OSC to have sat on the DOE report for six months. OSC has never provided me with a reason for the delay.

2. JUNE 2003: U.S. DOE OIG, Audit Report on "Management of the Department's Protective Forces," DOE/IG-0602;

3. JUNE 24, 2003: GAO Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform, NUCLEAR SECURITY: DOE Faces Security Challenges in the Post September 11, 2001, Environment," GAO 03-896-TNI

4. NOVEMBER 2003: U.S. DOE OIG, "Inspection Report on Reporting of Security Incidents at the Lawrence Livermore National Laboratory," DOE/IG-0625

5. NOVEMBER 2003: U.S. DOE OIG, Special Report on "Management Challenges at the Department of Energy," DOE/IG-0626

6. JANUARY 2004: U.S. DOE OIG, Inspection Report on "Protective Force Performance Test Improprieties," DOE/IG-0636

7. MARCH 2004: U.S. DOE OIG, Audit Report on "The Department's Basic Protective Force Training Program," DOE/IG-0641

8. NOVEMBER 2004: U.S. DOE OIG, Special Report on "Management Challenges at the Department of Energy," DOE/IG-0667

9. FEBRUARY 2005: U.S. DOE OIG, Inspection Report on "Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory," DOE/IG-0677

10. MAY 2005: "NNSA Security, An Independent Review," conducted by Richard W. Mies, Admiral USN (Retired), et al.

11. JUNE 2005: U.S. DOE OIG, Inspection Report on "Security Access Controls at the Y-12 National Security Complex," DOE/IG-0691

12. JUNE 2005: U.S. DOE OIG, Inspection Report on "Protective Force Training at the Department of Energy's Oak Ridge Reservation," DOE/IG-0694

I won't belabor the subcommittee by detailing point-by-point the evidence in each report which renders the DOE rebuttal to my disclosure inaccurate and meaningless. I provided the Office of Special Counsel with four detailed- sets of additional comments after the DOE report was submitted. Suffice it to say that I believe any objective and reasonable person evaluating my whistleblower disclosures, the DOE rebuttal concerning

my disclosures, and the subsequent, directly relevant reports cited above would find the DOE report seriously lacking in credibility.

The most telling examples come from one of the most recent, and in my opinion, the most comprehensive and credible of the reports listed above. The internal NNSA security review by Admiral Richard Mies (USN, Retired), concluded:

> **"Of greatest concern, our panel finds that past studies and reviews of DOE/NNSA security have reached similar findings regarding the cultural, personnel, organizational, policy and procedural challenges that exist within DOE and NNSA. Many of these issues are not new; many continue to exist because a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. Robust, formal mechanisms to evaluate findings, assess underlying root causes, analyze alternative courses of action, formulate appropriate corrective action, gain approval, and effectively implement change are weak to non-existent within DOE/NNSA.**
>
> **Accordingly, our panel strongly recommends that NNSA continue to work within DOE to develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations...**
>
> **NNSA has accomplished many of its stated goals...but its culture still reflects many of the long-standing negative attributes of DOE. NNSA is plagued by a number of cultural problems that, until addressed, will erode its ability to establish and provide security consistent with the gravity of its mission:**
>
> - **Lack of a team approach to security**
> - **Disparate views and an underappreciation of security across the enterprise, such that security is not full embraced as integral to mission.**
> - **Ingrained organizational relationships that inhibit an enterprise approach to security**
> - **A bias against training**
> - **An over-reliance on a compliance-based approach to security rather than a more balanced approach using performance-based standards**
> - **Lack of trust in the security organization**
> - **An absence of accountability."**

Juxtaposed with the analogous, now 6-year-old findings in the *1999* PFIAB Report quoted above, the conclusions in the Mies Report are deeply troubling. Along with these general conclusions, the Mies Report specifically corroborates many of the same critical issues I identified in my whistleblower disclosure almost 4 years ago, in some cases word for word. These include the lack of necessary qualifications of security personnel, a lack of centralized security oversight, a flawed vulnerability assessment and performance test process that provides "a false sense of security," and a general lack of protective force capability resulting in numerous exploitable vulnerabilities for a determined terrorist adversary.

An important illustration of this is DOE's unmistakable denial of an issue central to my whistleblowing: its post 9/11 failure to prepare for "worst-case" threat scenarios, such as suicide terrorist squads intent on detonating nuclear material, rather than stealing it. These "ssabotage" scenarios are far more difficult to defend against than theft because escape is not required, there is less exposure to protective forces, and the terrorists are assumed to be suicidal or willing to die. Still, the bottom line is that when national security is at stake, credible tests must be conducted and effective plans must be in place. DOE has failed to do this, instead denying that the most well-known terrorist tactic is a problem. Consider a directly related concern about inadequate recapture/recovery capability expressed in my OSC whistleblower disclosure (Feb. 2002), followed by DOE's documented dismissal of the concern in May 2003, and finally the Mies Report's findings on the exact same issue in May 2005:

Levernier OSC whistleblower disclosure, February 2002:

> "DOE consistently fails to performance test recapture recovery capability. When the adversary goal is to create an improvised nuclear device or radiological sabotage, escape is not required. Accordingly, DOE requires that all site protective forces possess the capability to reenter facilities under adversary control and recapture the asset. DOE Order 470.1 Chapter I, states, "Should denial and /or containment fail, a recapture/recovery or pursuit strategy would then be required. Forces shall be capable of rapid reaction in implementing recapture or recovery contingencies.
>
> This is a tactically difficult, high risk, operation that must be accomplished quickly, in order to deny the adversary time to complete their goal [i.e. the detonation of an improvised nuclear device!]....DOE's failure to test this

component of their protection strategy provides no assurance of adequate protection from this critical threat.

DOE requires that nuclear facilities possess the capability for mechanical and/or explosive reentry to assist in the timely interruption of an adversary force. Site Fire Departments (not protective forces) at two facilities are assigned this critical security responsibility. Other DOE facilities have not addressed this requirement and it has not been performance tested.

DOE should take immediate steps to ensure that recapture/recovery capability is performance tested at all facilities and ensure that recapture /recovery is tested routinely hereafter. DOE policy should be revised to require that recapture/recovery capability be performance tested annually, at a minimum."

DOE rebuttal to Levernier disclosure, May 2003:

"Due to deficiencies and gaps in the force-on-force performance exercises, the claimant alleges that DOE is not adequately prepared to defend the facilities against such an attack [i.e. detonation of improvised nuclear devise, dirty bomb]. According to the informant, these deficiencies violate DOE Order 470.1, which requires that the protective force be capable of rapid reaction in order to recapture a DOE asset or stop a sabotage attack.

All DOE sites have a recapture/recovery program as required by Departmental directives. The DOE sites test this recapture/recovery capability.

The claimant is correct in his observation that these types of activities are difficult and dangerous situations. The protection strategies for DOE sites are designed to prevent the site from being placed in a situation where recapture/recovery is needed. Thus, the focus of training is on ensuring that these conditions will not occur. However, DOE does run tests that presume the site has failed in its main goal and must, therefore, perform a recapture/recovery operation. The claimant is apparently not aware of the level of emphasis in these exercises, as several changes to the tactical protection strategies at DOE sites have been made based upon performance test results.

The recent testing by the Independent Oversight Office has placed increased emphasis on recapture/recovery, while still ensuring the major focus is on preventing a site from getting into a situation that would require this effort. These changes in tactical protection strategies, combined with additional training and oversight, have increased the level

of assurance that the DOE can successfully accomplish this difficult mission…

…DOE sites have demonstrated their ability to protect against this threat. The DOE is confident that its protective forces are capable of rapid reaction to implement recapture/recovery actions."

Finally, the findings of the independent Mies Report echo the allegedly dated claims, two years after DOE's dismissal, in May 2005:

"Site Recapture and Recovery (R&R) plans are nonexistent or inadequate. The sites explain that they focus on a denial-of-access strategy. Denial of access is the primary mission of NNSA sites, and resources and efforts should be dedicated to developing robust denial strategies. However, some sites' reliance on the viability of their denial strategies has precluded them from adequate planning, training, and procurement of appropriate tools for R&R should denial fail.

Some sites' R&R plans incorporate a denial-of-access strategy that inappropriately assumes they will never lose control of the facility. If adversaries gain access to a facility or leave with material, R&R programs are critical. Furthermore, the new DBT policy established site responsibility for instituting an R&R program.

SSSPs and some facility response plans address R&R programs and plans, but they vary widely, and some do not fulfill the need for a timely, effective, and viable R&R capability or meet the intent of DOE Manual 473.2-2. Some approaches include R&R response activities and requirements (spread throughout different response documents) but do not identify one specific response plan for R&R of an SNM storage facility or material in un-authorized control.

Other R&R approaches include tactical options that are rudimentary, very high risk, and not tactically viable. For example, the mechanical and electronic entry techniques used at some sites have not been performance tested or fully evaluated for their effectiveness, and, during iterative site analysis (ISA) processes or OA inspections; some of these techniques have failed testing. DOE Manual 473.2-2 states that when mechanical entry alone will not meet required response times, the site or facility must develop an explosive tactical entry capability...

Although the elements of response plan training and testing are critical to effective R&R programs, very few sites have conducted actual training or testing, and those that have use tabletop activities or walk-through drills.

> Adversary capabilities continue to increase, but NNSA threat planning lacks dedicated offensive response teams for each site to meet these threats. The manpower-intensive denial-of-access strategy requires numerous protective force personnel dedicated to a material access area in a repel-type posture. Sites say that the resources committed to this effort prevent them from assigning an offensive force as a dedicated, ready, and equipped element for R&R response activities."

I have attached a chart that compares similar DOE responses to my whistleblower disclosures with relevant sections in the Mies report. (attachment 2) Issues which the DOE determined were unfounded or dated two years ago still have not been addressed.

After wavering over DOE's denials for over two years, on February 2, 2006, OSC finally completed its review of my whistleblowing. Special Counsel Scott Bloch concluded in a letter sent to President Bush and to DOE's oversight committees in Congress, "The information [Levernier] presented casts doubt upon [DOE's] confident expression of its readiness to defend the nuclear research facilities and nuclear assets within its custody." (attachment 3) In essence, Special Counsel Bloch vindicated the overall substance of my whistleblowing. However, he refused to demand corrective actions from DOE. Moreover, he refused to even meet a requirement of the Whistleblower Protection Act to evaluate the DOE report, instead writing to the President that he is "unable to determine whether [DOE's] findings appear reasonable." The OSC is required by the WPA to reject an agency's report if it doesn't adequately resolve a whistleblower's complaint. My attorney at the Government Accountablity Project (GAP) tells me that this is the first time in GAP's experience monitoring the implementation of the WPA that a Special Counsel has failed to meet the statutory requirement to "determine whether the agency report is reasonable."

Conclusion

If DOE denies everything and the Special Counsel simply washes his hands, issues a press release, and looks the other way, where exactly is a whistleblower supposed to turn? The obvious answers must include Congress and the public. It is unlikely that DOE will ever abandon its longstanding approach of denial for any alleged security problems without some sort of congressional intervention and public pressure.

Congress needs to assure the freedom to warn for concerned individuals like myself who attempt to address security vulnerabilities. But, that will happen only as the exception if the whistleblower law continues to leave us defenseless against security clearance harassment even for unclassified disclosures of dangerous government mismanagement. Closing that Whistleblower Protection Act loophole would be an important step in providing genuine rights for those who take their national security responsibilities seriously.