DOE/IG-0482

I N S P E C T I O N R E P O R T

SUMMARY REPORT ON ALLEGATIONS CONCERNING THE DEPARTMENT OF ENERGY'S SITE SAFEGUARDS AND SECURITY PLANNING PROCESS

SEPTEMBER 2000

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

Department of Energy

Washington, DC 20585

September 28, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman /s/
Inspector General

SUBJECT: INFORMATION: Summary Report on "Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process" DOE/IG-0482

BACKGROUND

The Director, Office of Security and Emergency Operations provided the Office of Inspector General with a letter he had received which raised allegations of serious improprieties in the Department of Energy's Site Safeguards and Security Planning (SSSP) process. Specifically, the letter included allegations that a number of people within the Department were "lying in the reporting of the actual status of security" at the Department's most important nuclear sites, and that a contractor's findings under the SSSP Quality Assurance (QA) process were either ignored or not acted upon in a timely manner. In addition, it was alleged that "illegal" retaliation was taken against those who were trying to correct the Department's security problems through SSSP reviews or through assistance to a special assistant to the Secretary on Department security issues. The Office of Inspector General initiated an inspection to evaluate these issues.

RESULTS OF INSPECTION

While the inspection disclosed significant problems in the SSSP process as it was functioning at the time referred to in the allegations, the evidence did not support the principal points raised in the letter. Specifically, the inspection findings did not support the allegations that Department officials:

- lied in the reporting of the actual status of security at the Department's most important nuclear sites; or

- suffered retaliation for their part in the review of SSSPs, or for assisting a special assistant to the Secretary of Energy.

We did find that an employee of a support services contractor believed that an Office of Safeguards and Security program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA process and for assisting the special assistant to the Secretary. However, the program manager denied making such threats.

We did identify significant problems in the manner in which SSSPs were reviewed and SSSP QA issues were closed during the period referred to in the allegations. Specifically:

- There were substantial 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.

- Final Departmental decisions on how to address the SSSP QA issues were often complicated or delayed by disagreements between field and Headquarters elements over fundamental questions such as interpretation of the Design Basis Threat, adversary capabilities, and the assumptions related to worst case scenarios. These relationships were often so acrimonious as to threaten the effectiveness of the SSSP process.

- Since there was no process to resolve SSSP QA issues in coordination with the SSSP QA function, certain "Risk" issues remained unresolved at the SSSP QA level or were not fully evaluated.

The inspection disclosed that the allegations primarily concerned an SSSP process that has been phased out by the Department. The Office of Security and Emergency Operations is implementing a new process that is intended to address many of the problems that developed during past reviews of SSSPs. We concluded that the Department's restructuring of the SSSP process, if implemented and executed as planned, has the potential for resolving disagreements over the fundamental questions that affect SSSP "Risk" determinations.

This report includes several recommendations for the Director of the Office of Security and Emergency Operations: most notably, to establish a policy on what actions are required once high and moderate risks are identified through the SSSP process; and, to ensure that a dispute resolution process resolves disagreements that occur.

MANAGEMENT REACTION

The Director of the Office of Security and Emergency Operations stated that he had reviewed the Draft Report, and concurred. The Director stated that the conclusions offered in the Draft Report were appropriate. Although the Director has not committed to implementing the inspection recommendations, he stated that he would review the relevance of the recommendations in light of other policy initiatives currently underway to ensure that they are complementary. He also stated that if it is determined that the recommendations are appropriate and represent added value to the Site Safeguards and Security Planning Process, they will be implemented.

Attachment

cc: Deputy Secretary
Under Secretary for Nuclear Security/Administrator for National Security
Under Secretary for Energy, Science and Environment
Deputy Administrator for Defense Programs
Director, Office of Security and Emergency Operations
Director, Office of Security Affairs
Director, Office of Safeguards and Security
Director, Office of Defense Nuclear Security
Assistant Secretary for Environmental Management
Manager, Albuquerque Operations Office
Manager, Rocky Flats Field Office
Director, Transportation Safeguards Division
Director, Office of Security Support, Defense Programs

SUMMARY REPORT ON ALLEGATIONS CONCERNING THE DEPARTMENT OF ENERGY'S SITE SAFEGUARDS AND SECURITY PLANNING PROCESS

TABLE OF CONTENTS

Overview

INTRODUCTION AND OBJECTIVE

In January 2000, the Office of Inspector General received an allegation that there were serious improprieties in the Department's Site Safeguards and Security Planning (SSSP) process. Specifically, it was alleged that a number of people within the Department were "lying in the reporting of the actual status of security" at the Department's most important nuclear sites. Specific allegations were made regarding the Rocky Flats Environmental and Technology Site (RFETS), the Transportation Safeguards Division (TSD), and Los Alamos National Laboratory (LANL). In addition, it was alleged that "illegal" retaliation was taken against those who were trying to correct the Department's security problems through SSSP reviews or through assistance to a special assistant to the Secretary on Department security issues.

Based on these allegations, the Office of Inspector General initiated an inspection to determine if:

- officials within the Department were lying in the reporting of the actual status of security at the Department's most important nuclear sites;
- appropriate actions were taken to evaluate and resolve High Risk concerns;
- there was a systematic pattern of "dumbing" down the SSSP process; and,
- there has been retaliation against those who were trying to correct security problems.

As noted above, this inspection focused on the manner in which the contractor's concerns were addressed by Department security officials once they were raised. The issue of whether or not certain risk conditions actually existed at Department sites, as alleged, was beyond the scope of our review.

OBSERVATIONS AND CONCLUSIONS

REPORTING OF THE ACTUAL STATUS OF SECURITY

The Office of Inspector General found no evidence to support the allegation that Department officials lied in the reporting of the actual status of security at RFETS, TSD, and LANL. Contrary to this allegation, the results of our inspection revealed that Department officials took steps to assure that many of the SSSP QA issues reported by the contractor and the QA function were briefed at the highest levels of Department management.

However, a comparison of the SSSP QA analyses prepared by the contractor, and SSSP correspondence and documentation prepared and approved by the Department's Field and Headquarters Program Offices, did reveal substantial differences in what was being reported as the actual status of security at these three sites. We found that these differences were the result of significant, and, at times, bitter disagreements over the underlying basis of the SSSP QA issues raised by the contractor. The contractor's QA concerns were not well received at the Field Office level, the Program Office level, or by certain elements of the Office of Safeguards and Security. In several instances, the QA analyses performed by the contractor used different assumptions than had been used by the sites to develop their draft SSSPs, creating contention over the contractor's determinations of risk. The risk conditions identified and reported by the contractor were not universally accepted within the Office of Safeguards and Security or by the affected field sites and Program Offices.

ACTIONS TO EVALUATE AND RESOLVE HIGH RISK CONCERNS

Field and Headquarters elements considered and reviewed the QA issues identified by the contractor and the QA function. However, decisions on how to address the QA security concerns were often complicated or delayed by disagreements over fundamental questions such as interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that went into the identification, modeling, and testing of worst case scenarios. For example:

- The contractor and the QA function reported a High Risk concern at a RFETS facility in March 1997. The condition underlying the High Risk concern was not resolved at the QA level for nearly two and one-half years, and the corrective actions taken in October 1999 were still disputed by the site with regard to the necessity for these actions.

Many of the QA issues were briefed within the highest levels of Department management, yet we could not identify a systematic process for resolving and closing the QA issues in coordination with the QA function. As a result, certain issues remained

unresolved at the QA level or were not fully evaluated. For example:

- The contractor and the QA function reported two High Risk scenarios involving TSD operations during its review of TSD's draft September 1998 SSSP. However, the High Risk label was removed from the discussions on one of these issues, and the issue of High Risk in this case was never resolved with the QA function. The Office of Safeguards and Security and TSD did agree to address many of the underlying security concerns that contributed to the QA assertion of High Risk.

- During a limited review of LANL's draft 1999 SSSP, the contractor and the QA function reported that SNM was not at low risk at a LANL facility. However, the issues identified in the contractor's final SSSP QA analysis were not forwarded to the Albuquerque Operations Office or the site for evaluation prior to SSSP concurrence by the Office of Security Affairs.

NO EVIDENCE OF "DUMBING" DOWN THE SSSP PROCESS

We concluded that the "new" SSSP procedures being implemented by the Office of Security and Emergency Operations did not reflect a systematic pattern of "dumbing" down the SSSP process. In fact, we concluded that the new SSSP procedures have the potential for significantly enhancing the SSSP process. Nevertheless, given the Department's past experiences in the security area, strong management involvement will be needed to assure that the "new" process achieves its potential. The Secretary of Energy assigned this role to the Director, Office of Security and Emergency Operations, in June 1999, and stated that the new Director has "the experience, expertise and determination to change the security culture at DOE." This role will have to be re-evaluated in light of the establishment of the National Nuclear Security Administration.

The Department began restructuring the SSSP process in May 1999. The Office of Safeguards and Security believed that the "old" SSSP QA process caused a great deal of contention when Headquarters Offices performed "a post-facto" verification and validation exercise using tools or approaches different than those used to perform the initial risk assessment by the sites. In May 1999, the Under Secretary directed that an SSSP Working Group be formed to provide "new" detailed procedures for the development and approval of SSSPs. The most significant changes from the "old" to the "new" SSSP process was the introduction of a "participatory approach" to the preparation of the SSSPs. The "participatory approach" involves field elements and various Headquarters offices in the SSSP development from the beginning,

eliminating the need for a "post-facto" QA function. Under the "participatory approach," agreement is to be reached on the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios early in the process, thereby avoiding the introduction of different interpretations and assumptions at the end.

The "new" process also introduced a different approach to "Risk." Under the new process, "risk avoidance" was replaced by the concept of "risk management." As described to us, the "new" process emphasizes the necessity of a common, up front agreement on factors that are absolutely critical to the structure of the protection systems designed to counter adversary acts. We concluded that the "new" process must not only move the discussion on the Design Basis Threat, adversary capabilities, and worst case scenarios to the beginning of the SSSP process, but must also provide for the resolution of disputes on these issues when they occur. We also concluded that the "new" process can be most effective if the "Risk" determinations are driven by a consensus within the Department on the interpretation of the Design Basis Threat, adversary capabilities, and worst case scenarios rather than based on the preferences of a single site and/or a Program Office. The Director of the Office of Safeguards and Security told us that "this will be the case."

The inspection disclosed that the "new" process appears to be evolving in a way that will address disputes and the factors affecting "Risk." For example, a newly formed Threat Assessment Quality Panel has assumed responsibility for matters relating to the Design Basis Threat, and any issues not resolved by this panel will be raised to the Security Management Board.[1] In addition, the Threat Assessment Quality Panel has recently issued guidance to Department sites regarding the applicable adversary capabilities under the specific elements of the Design Basis Threat.

The "new" process was first used in April 2000 for the 2000 TSD SSSP. We have not evaluated the effectiveness of this process.

RETALIATION

We found no evidence of retaliation as alleged with respect to Department officials. Interviews of Department officials who were alleged to have been retaliated against for their part in the review of SSSPs, or for assisting a special assistant to the Secretary of Energy on security issues, did not support the allegation of retaliation. However, one support services contractor believed that

[1] The Security Management Board was abolished in October 1999, and a new organization to take over its responsibilities has not been established.

an OSS program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA process and for assisting the special assistant. The contractor said that he did not receive any contract work in the area of field assistance after the alleged threat was made, and that he viewed the elimination of his field assistance activities as retaliation. However, the OSS program manager denied any retaliation and said that he had no opportunity to provide contract work to this individual during the period in question. Subsequently, the contractor received other contract work, including work from the Director, Office of Security and Emergency Operations, and did not seek to formally address any concerns about alleged retaliation.

We also found no evidence that another support services contractor was retaliated against. The contractor offered a reduction in billable hours as evidence that the contractor was being retaliated against. However, while some Office of Safeguards and Security officials expressed dissatisfaction with the contractor, the use of the contractor by the Office of Safeguards and Security has continued. Office of Safeguards and Security records show that the contractor's billable hours had dropped off significantly in one area, but a review of the contractor's total direct productive labor hours over the past year showed only a slight decline in the overall use of the contractor by the Office of Safeguards and Security.

The evidence shows that the Department's shift from the "old" to the "new" SSSP process, and not retaliation on the part of any OSS official, more likely than not was the cause of this decline. The shift from the "old" to the "new" SSSP process nearly eliminated this company as a support services contractor. However, the contractor's direct productive labor hours have been sustained close to previous levels by providing support in other security areas.

Recommendations

We recommend that the Director of the Office of Security and Emergency Operations:

1. Establish policy on what actions are required once High Risk and Moderate Risk are identified through the SSSP process, including the resolution of High Risk and Moderate Risk issues within specific timeframes; and the consideration for compensatory measures, formal acceptance of risk, and mitigation of risk through operational changes.

2. Ensure that a dispute resolution process is incorporated within the responsibilities of the Threat Assessment Quality Panel and the successor organization to the Security Management Board so that disagreements on the interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios are addressed at the highest level of management.

3. This recommendation is classified.

4. Ensure that TSD validates the Special Response Force through the use of performance testing of the worst case scenarios.

5. Evaluate TSD's performance testing program and assure that all performance tests used to validate their SSSPs (a) are not encumbered by training priorities, (b) constitute legitimate force-on-force activities without coaching by instructors/controller, and (c) provide results that are conclusive in terms of measuring the ability of Special Agents to perform in response to an actual attack.

6. Ensure that TSD validates all other corrective actions that were identified on the "TSD Interim Disposition of NN Comments" matrix.

7. Ensure that TSD identifies a site suitable for conducting force-on-force exercises for worst case scenarios.

8. Evaluate the concern that a "Super Adversary" is created by the application of the Design Basis Threat to worst case scenarios, and determine what action is needed to disseminate more prescriptive policy on adversary capabilities so that the threat and adversary attributes contained in the Design Basis Threat are clear, concise and universally understood by the Office of Security Affairs, Office of Independent Oversight and

Performance Assurance, the Program Offices, and all affected field elements.

It should be noted that certain recommendations originally sent to the Director, Office of Security and Emergency Operations for comment are now the responsibility of the Under Secretary for Nuclear Security/Administrator for National Security.

MANAGEMENT COMMENTS

Officials from the Office of Security and Emergency Operations provided several comments to the initial Draft Report dated July 21, 2000. Appropriate changes were made based on these comments, and a second draft report was issued on August 31, 2000.

In comments provided to the second Draft Report, the Director of the Office of Security and Emergency Operations stated that he had reviewed the Draft Report, and concurred. The Director stated that the conclusions offered in the Draft Report were appropriate, and that it appeared that most of the comments provided by members of the Office of Security and Emergency Operations on the initial Draft Report had been incorporated into this version.

While the Director did not commit to implementing the recommendations, he stated that he would review the relevance of the recommendations in light of other policy initiatives currently underway to ensure that they are complementary. He also stated that if it is determined that the recommendations are appropriate and represent added value to the Site Safeguards and Security Planning Process, they will be implemented. In addition, the Director stated that he would forward to the National Nuclear Security Administration, Office of Defense Nuclear Security, those recommendations that fall under their purview.

INSPECTOR COMMENTS

Since the Director of the Office of Security and Emergency Operations did not specifically concur or non-concur with the report recommendations, we believe it is critical that the Director's initial submission under the Department's Audit Report Tracking System (DARTS) clearly defines the rational for determining that any of the recommended actions are not appropriate or do not represent added value to the Site Safeguards and Security Planning Process. In addition, the Office of Security and Emergency Operations, in coordination with the National Nuclear Security Administration, should clearly define their plan for corrective actions in their initial submission under DARTS.

Appendix A

SCOPE AND METHODOLOGY

While reviewing the allegations discussed in this report, we evaluated:

- The reporting of the status of security at RFETS, TSD, and LANL through the SSSP process.

- The appropriateness of the actions taken by Department management to evaluate and resolve High Risk concerns identified by the contractor and the SSSP QA function.

- The appropriateness of the actions taken by Department management to evaluate and resolve other security weaknesses identified by the contractor.

- Changes to the SSSP process that eliminated the post-facto SSSP QA reviews.

- The issue of retaliation as it related to certain Department and contractor employees who were involved in the SSSP QA process.

As part of our review, we interviewed officials from the contractor organization, Los Alamos National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Department officials from the Office of Security and Emergency Operations, the Office of Safeguards and Security, the Office of Security Affairs, the Office of Defense Programs, the Office of Environmental Management, TSD, and the Albuquerque Operations Office.

In addition, we also reviewed documentation relating to the SSSP QA process, including: (1) SSSPs for TSD and LANL; (2) SSSP QA reports, including ALPHA Reports, Physical Security Systems Reports, an Integrated Report for TSD, and JTS Reports; (3) a Format and Content Guide for SSSPs; (4) Acceptance Criteria and Review Guide for SSSPs; (5) a Final Report of the Design Basis Threat Working Group and the SSSP Working Group; (6) the SSSP Rollout 2000 Workshop Report and the Tool Box Evaluation; (7) the Vulnerability Assessment Program Workshop Report; and (8) applicable Department of Energy Orders and Directives regarding security at Department sites.

This inspection was performed between January and June 2000. This inspection was conducted in accordance with the "Quality Standards for Inspection" issued by the President's Council on Integrity and Efficiency.

Appendix B

BACKGROUND

The SSSP describes safeguards and security programs and vulnerability and risk analysis at applicable sites. The SSSP is the primary instrument that the Department's Operations Office Managers use to certify to the Secretary of Energy the accuracy of risk and the measures used to assure that the public, employees, environment, and national assets are adequately protected. The SSSP is approved by Heads of Field Elements and concurred in by the cognizant Program Office and the Office of Security Affairs.

All SSSPs are to be certified annually as being current and valid, and are to be updated and approved at least once every five years unless a more frequent cycle is warranted. The Operations Office/Field Office Manager, in consultation with the Program Offices, Office of Independent Oversight and Performance Assurance, and the Office of Security Affairs, can direct that the SSSP be updated to reflect evolving threats and changes in a site's security posture.

In 1997, the Office of Nonproliferation and National Security began what they called "a rigorous and disciplined" QA process as part of the "review and verification" of the Department's SSSPs (referred to as the SSSP QA process). The Office of Safeguards and Security had found significant deficiencies in reporting "Risk," often due to the characterization of the Design Basis Threat and scenarios that did not stress the worst case. During this period, the Office of Safeguards and Security assigned the contractor the task of supporting the SSSP QA effort.

In an August 21, 1997, memorandum to various OSS Division Directors, the Director of OSS issued criteria and methodology that would be employed in the reviews of SSSPs. The purpose of this criteria and methodology was to address systemic SSSP verification issues that had arisen during prior reviews.

The SSSP QA process employed the use of three specific tools for review and verification of the Department's SSSPs. These included:

- Joint Tactical Simulation (JTS) - an interactive, entity-level conflict simulation modeling tool;
- Advanced Logic Protection Heuristic Analysis (ALPHA) - a vulnerability assessment tool; and,
- Physical Security Systems Reviews (PSSRs) - examinations, tests, and evaluations of the effectiveness of physical security systems.

In a November 4, 1998, memorandum to the OSS Acting Director, Field Operations Division, the OSS Director stated that he considered the reviews of SSSPs to be a "critical principle" function of OSS. The Director stated that the three "primary tools" used, ALPHA, JTS, and PSSRs, must be carefully integrated and appropriately documented for each SSSP. The Director also stated that it was expected that each of these tools would be used to evaluate all SSSPs unless timely equivalent information existed. The Director recognized that a "constructive tension condition" existed between the Safeguards and Security office responsible for the SSSP QA process and the Safeguards and Security office responsible for field assistance and expediting OSS concurrence with SSSP's. However, he stated that these checks and balances would result in a more effective safeguards and security program.

As part of its support role associated with the SSSP QA effort, the contractor reported that High Risk security conditions existed at the Rocky Flats Environmental Technology Site, and the Transportation Safeguards Division. Further, with regard to Los Alamos National Laboratory, the contractor concluded that "there is insufficient evidence to provide reasonable assurance that SNM [Special Nuclear Material] is protected to the standard required by the Department. . . . That is, SNM is not at low risk . . . ."

The contractor alleged that findings at these three sites were either ignored, or not acted upon in a timely manner. For example, it was alleged that the contractor identified High Risk at RFETS in March 1997, but no action was taken to address the High Risk condition until November 1999. Also, the contractor allegedly identified High Risk conditions involving TSD operations in the fall of 1998 that were never addressed, and that allegedly remain today. In reviewing the LANL SSSP in November 1999, the contractor allegedly found major problems with the ability of the protective force to deal with worst case scenarios that were never addressed, and also allegedly remain today. The contractor also alleged that the SSSP QA review process is currently being restructured, and that documents for this effort show a systematic pattern of "dumbing" down the SSSP process. The contractor explained that the SSSP QA process is being subverted so that SSSP development becomes a joint Field/Headquarters function with no independent review.

Appendix C

DEFINITIONS

Risk	Risk is defined as Low, Moderate, or High. Risk ratings are determined by evaluating the effectiveness of the protection system against events such as the threat of the theft of Special Nuclear Material (SNM), weapons, and weapons components. Department policy states that Low Risk Ratings are acceptable.
Design Basis Threat	The Design Basis Threat is a postulated threat used to design protective forces and security systems for the guarding of nuclear sites. The Design Basis Threat describes the most credible and serious potential adversaries, their tactics, numbers, and capabilities. The purpose of the Design Basis Threat is: (1) to provide a stable basis for security planning and budgeting that is predicated on a predetermined threat estimate which is not dependent on tactical intelligence, (2) to provide a baseline for DOE-wide protection standards for our most attractive nuclear assets, and (3) to provide a standard against which to evaluate the performance of protective forces and the effectiveness of installed security systems.
Verification and Validation	Verification is accomplished through the conduct of vulnerability assessments, use of modeling tools, evaluation of training and maintenance records, and table-top exercises of varying degrees of formality. Validation is a process where assumptions reached through assessments, modeling and evaluation activities are tested for validity, the predominant tool utilized being the performance test (ranging from tests of an individual's skills to a full scale force-on-force exercise).

IG Report No. DOE/IG-0482

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we nay any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.