NUREG-0095
ERDA 77-34

JOINT ERDA-NRC TASK FORCE ON SAFEGUARDS

Final Report
July 12, 1976

[Unclassified Version]

Manuscript Completed : November 1976
Date Published : February 1977

U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

U. S. Energy Research and Development Administration
Washington, D.C. 20545

JOINT ERDA/NRC TASK FORCE ORGANIZATION

Steering Group

Kenneth R. Chapman, Director, Office of Nuclear Material Safety and Safeguards, NRC

E. B. Giller, Deputy Assistant Administrator for National Security, ERDA

Task Force Director

Carl H. Builder, Director, Division of Safeguards, NRC

Full-Time Staff

NRC	ERDA
Richard C. Lyons	Leonard M. Brenner
Stephen K. Conver	William C. Bartels
David B. Matthews	
Bonnie Sue Palmer	

The task force appreciates the direct assistance and helpful suggestions of many other members of the ERDA and NRC staffs.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

On March 12, 1976, the responsible managers from ERDA and NRC met to review the status of safeguards investigations then in progress at certain nuclear fuel cycle facilities licensed by the NRC which process nuclear materials under ERDA contracts. This meeting resulted in the creation of a joint ERDA-NRC task force to develop a proposed action plan for improving the control and protection of nuclear materials at NRC licensed fuel cycle facilities possessing significant amounts* of high enriched uranium and plutonium. This report briefly summarizes the task force findings and proposed plan of action.

The task force addressed the current status and future direction of physical security safeguards at NRC licensed fuel cycle facilities now in possession of significant amounts of strategic special nuclear materials (SSNM).** The focus of the task force was on near-term, site specific actions that would provide confident control and protection against thefts or diversions of SSNM.

STATUS OF CURRENT SAFEGUARDS

In January 1976, the NRC began a special review of the safeguards maintained by fuel cycle licensees who possess significant amounts of high enriched uranium and plutonium. In March, ERDA began participating in those reviews. Onsite evaluations were made to assess the effectiveness of programs

---

* Two kilograms of plutonium or five kilograms of uranium-235 (contained in uranium enriched to more than 20 percent in the U-235 isotope).

**Plutonium, uranium-233, or uranium enriched to 20 percent or more in the U-235 isotope.

approved and implemented to meet current regulations and to judge safeguards capabilities against specific threat levels. The capabilities of 13 licensees (involving 15 facilities) were examined. The threat levels defined for this review consisted of:

- an internal threat of one employee occupying any position, or
- an external threat comprised of three well-armed (legally obtainable weapons), well-trained individuals, including the possibilities of inside knowledge or assistance of one insider.

The same threat criteria were applied during a comparative review conducted at three representative ERDA facilities to assess the parity of safeguards between NRC-licensed and ERDA license-exempt facilities.

The site reviews indicated that the licensees were generally in compliance with NRC safeguards regulations. Nevertheless, it was found that improvements would be needed at each of the facilities in order to assure a capability to counter the threat levels defined for this review. The required improvements are now being accomplished by the imposition of more specific or additional license conditions on a case basis. The most prevalent shortcomings noted were those related to the control of access to SSNM (both stored and in process), exit search procedures, and onsite and offsite response capabilities.

Systems and procedures required for protection against threats consisting of one employee acting alone or with three well-armed, well-trained attackers are generally consistent with the current systems and procedures required in 10 CFR Parts 70 and 73. However, threat levels are not specified in the

current safeguards requirements as a basis for either design or evaluation. The need for improvements to meet the threat levels defined for this review may be attributable, in part, to the fact that such performance criteria had not been previously defined nor imposed upon industry as a safeguards requirement.

Of the 15 NRC licensed facilities involved in the safeguards reviews, eight facilities are now judged to be adequate to withstand both the external and internal threats defined for the review. Of the remaining seven, one is judged adequate to protect against the external threat, but not the internal threat; four are judged adequate to defend against the internal threat but not the external threat; and two are judged inadequate against both threats. Improvements at these facilities are being made by a combination of voluntary actions on the part of the licensees and government directed actions. Completion of these actions is expected by August 1976.

Although specific actions have been directed on a site-by-site basis, this approach may not sustain a performance level compatible with the currently desired posture unless the licensees are informed of the criteria for that posture and accept an obligation for maintaining the required safeguards capabilities.

Conclusions from the comparative evaluations at three ERDA facilities were:

- Present capabilities are more than adequate against the unassisted external threat levels assumed in this review.

- The facilities could not, with a high degree of assurance, protect against an external force in possession of inside knowledge or assistance and operating in a covert manner because of inadequate, marginally effective detection aids.
- One facility could not, with a high degree of assurance, prevent the diversion of significant quantities of SSNM by an insider. Improvements were needed at all three facilities in the techniques used to prevent the diversion of significant quantities of SSNM.

As an interim measure, short-term improvements have been made since the assessment at each of these facilities. They are presently judged to have the capability for countering the external or internal threat levels used as review criteria.

SAFEGUARDS POSTURE CONSIDERATIONS

The Threat

There is no evidence available to ERDA or NRC to indicate any imminent threat of theft or diversion of SSNM. No persons or groups have been identified as posing an apparent threat to steal SSNM, nor has any black market been identified as a motivation for theft of SSNM. The most plausible incentives for the theft or diversion of SSNM appear to be the possession of nuclear materials for the purposes of extortion, ransom, or public attention.

In the absence of specific evidence of threats, safeguards planning must necessarily be based upon hypotheses of motivations and estimates of capabilities. The primary determinants of threat capabilities for theft are the

numbers of persons involved, their access to positions of trust with respect to SSNM, the availability of arms or special equipment that might facilitate a theft, and their willingness to sacrifice lives to achieve success.

Historical data on the numbers of persons involved in groups committing robberies, assaults, and acts of terrorism in this and other countries show that small groups predominate. Groups larger than six persons account for only a few percent of the cases, although there are isolated instances of very large groups. However, the relevance of this historical data to the future or to threats involving the theft of SSNM is problematical except as a point of departure.

Case studies of elaborate crimes or "capers" indicate that group size and composition are dictated by the demands of the job and not by the availability of people. Such crimes are generally characterized by careful planning and avoidance of violence. There is some evidence to support the notion of an inverse correlation between group size and the degree of planned violence.

The possibility of insiders participating in or instigating the theft of nuclear materials is considered by many to be more likely than an armed assault by outsiders. Thefts in commerce frequently involve insiders, and internal conspiracies are not uncommon in the hijacking or diversion of commercial freight.

The availability of sophisticated armaments to individuals or criminal groups is changing rapidly. Automatic rifles and plastic explosives are now widely available. Modern, high-technology weapons, such as wire-guided and

heat-seeking missiles, recoilless cannons, helicopters, etc., cannot be excluded as possibilities even though they may be unlikely based upon current evidence.

Thus, the evidence of current threat capabilities points toward the possibilities of more than a single insider acting alone or with a small group of persons armed with legally obtainable weapons.

Posture Issues

With respect to internal threats, high-confidence protection against any single insider, regardless of position or clearance, would appear to be a minimum safeguards posture. The current industry approaches that capability, with some exceptions as previously noted. The most vexing problem for the industry will be insuring against the insider being a key individual in the security organization.

If the protection against inside threats is expanded to include internal conspiracies, several important issues arise. One is the question of the effectiveness of personnel clearances based on full-field investigations in preventing criminal conspiracies. These are widely used in many of our national institutional arrangements; including the control over nuclear weapons. Similar clearance procedures, based upon full-field background investigations, can be applied to industry employees to reduce the likelihood and effectiveness of internal conspiracies for the purposes of theft or diversion of SSNM.

Systems and procedures can be installed within industrial facilities to protect against internal conspiracies, but they probably will require additional people, interfere with process operations, and necessitate physical rearrangements or additional security equipments in some plants. It may be operationally impractical to design such measures to be completely effective against conspiracies involving key management and security personnel. Thus, reliance upon personnel clearances may be necessary for key personnel. Nevertheless, prudent safeguards system design would make maximum use of technology and procedures to prevent conspiracy wherever practicable, even where personnel have been cleared. In any event, clearances should not be deemed adequate insurance against the theft of SSNM by any single insider, regardless of position or trust.

With respect to external threats, high-confidence protection against robbery by a small group of about three persons with inside assistance and armed with legally obtainable weapons would appear to be a minimum safeguards posture. The current industry meets or exceeds that capability with some exceptions as previously noted.

If the protection against external threats is expanded to include armed assaults by either (or both) larger group sizes or heavier arms, several important issues arise. A fundamental issue is whether the industry safeguards posture should be extended to encompass the threat of determined violent assaults. There is considerable reluctance expressed by some in industry to accept this responsibility, since it is beyond the scope of normal

industrial security. Several licensees profess to be sufficiently concerned to consider withdrawing from activities involving SSNM. If the industry safeguards posture must be upgraded against the threat of determined violent assaults, then it is evident that there is some level of force beyond which high-confidence protection cannot be provided by any practical means within current institutional arrangements. With group sizes substantially in excess of about six persons and with arms much beyond automatic rifles, almost any entity in the nation may be considered susceptible to a determined violent assault.

Insuring the protection of facilities against determined violent assaults with automatic small arms and explosives for breaching barriers will require substantial changes in the current industrial facilities. These would include greatly enlarged and better armed and trained guard forces, additional barriers, alarms and protected guard positions. Such additions would involve substantial capital and operating costs; alter the appearance of the plants toward that of military reservations; and would elevate concerns over a number of legal or policy issues concerning the rights, duties, and liabilities of guards.

MAJOR ISSUES AND ALTERNATIVES

The upgrading of physical security at licensed nuclear fuel cycle facilities will require a set of decisions relating to threat definition, the schedule and approach to upgrading, public disclosure of government intentions,

financing arrangements, and the regulatory means that will be used to achieve the upgrading. The issues involved are not easily isolated; they are so interwoven that a decision on any single issue is likely to bound the choices available in one or more other issues.

Definition of internal and external reference threat levels for design and evaluation is a fundamental issue. The principal question is the desirability of extending the current safeguards posture to protect against internal conspiracies or determined violent assaults. While both the internal and external threats can be characterized in a variety of ways using a number of variables, there appears to be a threshold between threats of a single insider and internal conspiracy. Similarly, a fairly clear distinction exists between external attacks characterized as professional armed robberies and those that may be described as determined violent assaults. These thresholds on internal and external threats define the two primary threat alternatives. A decision to maintain a safeguards posture that is effective against the lower threat levels has few impacts other than the need to codify the requirements.

If a decision is made to move to higher levels of protection, the implementation of that decision will be both difficult and time-consuming. If scheduled for completion using normal, routine procedures, the upgrading could require up to four years. The minimum time required without resorting to emergency methods is estimated at about two years. This minimum time would permit no more than about six months for the government to prepare the

necessary regulatory, financial, and design bases for the upgrading. The upgrading probably cannot be achieved in minimum time without extraordinary effort, including immediately effective rules or license conditions, several months of intense effort developing the information that the licensees will need to design their upgraded safeguards, some arrangement for financing safeguards costs, and some risks of companies withdrawing from business involving SSNM. An assessment of the environmental impact would be required to ascertain whether an environmental impact statement would be required.

Interim measures can provide an enhancement of safeguards prior to completion of a longer, more comprehensive upgrade program. The specific measures which are candidates for interim action are: institution of clearances for key personnel, improvements in guard armament and training, and some increases in guard numbers. Any additional interim measures take on the character of emergency actions that would go beyond those desired in an efficient, long-term solution.

Another important issue is the extent to which the government makes the objectives, threat specifics, and schedule of any upgrading program known to the licensees and the public. If the government initiates a major upgrading of safeguards without fully disclosing its programmatic intentions, the licensees will almost certainly contest what they perceive to be a ratcheting process without goals or limits. Declaration of the intent and specifics of the planned upgrading should result in acceptance by most licensees. However, several of the licensees, notably the larger more diversified companies, have

expressed the view that defending against determined violent assaults is more properly a governmental, not a private, function.

Most of the licensees express concern about the financial impacts of additional safeguards upon their domestic and international competitiveness. They appear to be particularly concerned with the capital costs for added safeguards. For ERDA contractors, capital expenditures for safeguards can be compensated through some form of initial financing support or later reimbursement of the licensees for depreciation of capital improvements for safeguards purposes. For several contractors, ERDA expects existing authority to be adequate for the financial impact of upgraded safeguards although additional funding may be needed. A more troublesome issue may be the question of government financing arrangements for licensees whose work is not entirely for ERDA. If initial financing is not made available to such vendors, or if adequate financing is not available to all licensees, industry-initiated court actions challenging the need or propriety of the upgrading should be expected.

Regulatory issues will arise in the procedures chosen for implementing any significant upgrade in safeguards. A decision must be made whether to impose the upgrading requirements by rulemaking, specific license conditions, or other means. Also, the government must decide if the upgrading of safeguards should be pursued within existing legal authority of licensees on use of force, types of armaments permitted, and other aspects of guard performance. A legislative change in these authorities would necessarily be a long-term

action. While some changes in the legal authority of licensee guards would undoubtedly improve their cost-effectiveness, such changes are not now seen as essential to an adequate safeguards posture.

RECOMMENDATIONS

Recommendations - Current Level of Safeguards

The task force recommends that both ERDA and NRC take the necessary near-term actions to establish and then consolidate a safeguards posture for licensed facilities that will afford high-confidence protection against theft of SSNM by a single insider acting alone or by a small, lightly armed group of outsiders. These actions should include:

- Completion of the ongoing specific improvements identified by the ERDA and NRC site reviews.
- Establishment of functional capabilities expected of safeguards systems and procedures for the protection of SSNM, including explicit descriptions of the threat levels and criteria to be used in evaluating their performance.
- Follow-up performance reviews to assure that the required improvements have been accomplished and that the desired levels of safeguards capabilities are being maintained.

These actions should be scheduled for completion before the end of summer. The task force recommends that follow-up reports on the state of the safeguards posture for the protection of SSNM at licensed fuel cycle facilities be submitted in the fall of this year.

Recommendations - Upgraded Safeguards

The task force recommends initiating actions to upgrade the safeguards posture to a level affording high-confidence protection against theft of SSNM by internal conspiracies or determined violent assaults. This recommendation is not based upon a perception of imminence of threats to the nuclear fuel industry; rather, it is based upon the judgment of the task force as to what constitutes a prudent level of protection. Some persons may feel that the current level of protection is adequate; others certainly would not be satisfied without levels of protection greater than those recommended. The task force believes that the upgrading of safeguards to these capabilities should be implemented as rapidly as possible, consistent with sound technical and policy decisionmaking. In the absence of evidence of serious threats to the industry, the task force does not believe that emergency measures, such as shutdown of the industry or the immediate use of federal forces, is warranted. On the other hand, the volatility of the threat situation with respect to the nuclear industry and society suggests that upgrading should be accomplished more quickly than by normal routine action.

The task force recommends that:

- NRC initiate within six months the following interim measures to upgrade safeguards:
  - Institute a program of clearances based upon full-field background investigations for selected licensee employees who might effectively conspire to steal or divert SSNM.

- Require licensee guards to be armed with semi-automatic rifles.
- Define and require a training program for licensee guards to insure an adequate knowledge of their duties and responsibilities.
- Insure that all licensees have sufficient numbers of guards to defend against attempted robbery by small groups of persons.

• NRC complete the following actions within six months:

- Resolve the need for employment constraints, if any, and establish requirements for the employment qualifications of guards whose duties include defense against determined assaults.
- Determine the utility of automatic weapons in the defense of nuclear facilities and, if judged necessary, initiate appropriate measures to permit their use by licensees.
- Make an initial environmental impact assessment for the proposed upgrading program.
- Establish, using the most expeditious regulatory means, the requirement to defend against internal conspiracies and against determined violent assaults.
- Establish methodology and procedures for inspecting and enforcing the performance requirements.
- Provide the means for each licensee to have access to classified information pertinent to the protection of their facilities.

- ERDA and NRC:
  - Disclose the intent to upgrade safeguards within two years to defend against both internal conspiracies and determined violent assaults.
  - Complete within 12 months the review and approval of all necessary facility modifications and security plans for upgraded safeguards, including cost estimates.
- The potential impacts of capital expenditures required to upgrade safeguards be carefully considered for all licensees, including those without ERDA contracts.

I. INTRODUCTION

As directed by the Administrator of the Energy Research and Development Administration (ERDA) and the Chairman of the Nuclear Regulatory Commission (NRC), a proposed action plan has been prepared for improving the control and protection of nuclear materials at commercial facilities possessing strategically significant amounts* of high enriched uranium and plutonium. This proposed action plan has been prepared by a joint ERDA-NRC task force during the period from March 17 to May 17, 1976. This report summarizes the task force activities and recommendations.

Background

On March 12, 1976, the Administrator, ERDA, and the Commissioners, NRC, along with senior members of their staffs, met to review the status of safeguards investigations and evaluations conducted by the NRC during the previous three months. This review highlighted what appeared to be chronic difficulties at several facilities in meeting the NRC accountability requirements, as well as weaknesses in nuclear materials control and protection procedures as practiced by several facilities under current NRC regulations. While accountability problems were most evident at bulk processing facilities handling large quantities of materials for ERDA contract programs, the nuclear materials control and protection at most commercial facilities handling highly enriched uranium or plutonium was judged to be less than that desired by both ERDA and NRC.

*Two kilograms of plutonium or five kilograms of uranium-235 (contained in uranium enriched to more than 20 percent in the U-235 isotope). The significant quantities for special nuclear materials are established at a level judged to be substantially less than that required for the illicit manufacture of a nuclear explosive.

The Administrator and Commissioners responded to this review by directing their staffs to initiate prompt action to improve the nuclear materials control and protection at the so-called mixed facilities (commercial facilities licensed by NRC and active or potential contractors to ERDA) which now possess about 99 percent of the high enriched uranium and plutonium in the commercial sector. It was agreed that the security of these materials was of utmost importance and that an action plan for improving physical security at mixed facilities should be formulated by the middle of May 1976. It was further agreed that the attention and assistance of industry was essential to the success of this effort and that the level of safeguards should be comparable at ERDA and commercial facilities. Finally, it was observed that the government, through its ERDA contracts, should share some equitable part of the economic burdens which might be imposed on its vendors by additional safeguards requirements arising from this action plan.

Task Force Scope

On March 17, 1976, a joint ERDA-NRC task force was formed and charged with developing, in coordination with industry, an action plan to assure confident control and protection of significant amounts of strategic special nuclear materials* (SSNM) under government regulations and contracts. The task force was directed to give first priority to near-term site-specific actions that would provide confident control and protection against thefts or diversion of SSNM at mixed facilities. The task force also was to consider

*Plutonium, uranium-233, or uranium enriched to 20 percent or more in the U-235 isotope.

commercial facilities that might possess SSNM under ERDA contracts in the future and longer term actions that might be required. By direction, however, material accountability measures, SSNM transportation security, and other threats such as sabotage, were excluded from consideration. Material accountability improvements, while possible and desirable, were judged to be longer term solutions, dependent upon the state-of-the-art in measurement and nondestructive assay techniques, and difficult to implement in some of the existing facilities without extensive modifications to the plant processes. In addition, there is some question whether any accountability method or system can contribute to improved physical protection of SSNM at facilities with high process or fabrication rates. Transportation security for SSNM was excluded because plans have been made to transport all government-owned SSNM by the ERDA transportation and courier system commencing in the fall of 1976, and further inquiry by the task force would have been overshadowed by that impending action. Furthermore, both material control and transportation security were being addressed separately under other ERDA and NRC planning activities. The security against theft of SSNM was emphasized because of the relative severity of its potential consequences.

The task force action plan was to include both generic and site-specific measures for improved safeguards, the impacts of these measures upon ERDA contracting and NRC regulatory activities, and a time-phased plan for implementing these measures. The task force was encouraged to solicit the assistance of industry in identifying and evaluating site-specific safeguards measures.

The resources of both ERDA and NRC were made available to the task force through their respective safeguards organizations. The NRC has the overall responsibility for regulating all facilities and materials licensed under the Atomic Energy Act and has the specific responsibility for establishing and maintaining adequate safeguards for the protection of commercial nuclear facilities and materials. As the principal customer of the licensees, ERDA responsibility extends to production performance and costs. ERDA responsibility includes assurance that increased payments to the licensees for safeguards are effectively spent and correctly attributed to safeguards because, ultimately, the increased costs are reflected in the price the government must pay for goods and services.

Twelve companies participated in the task force planning efforts (Table I-1). One of the companies, an NRC licensee, does not currently possess SSNM. The remaining 11 companies are involved with 13 organizational entities licensed by the NRC and are presently processing strategic special nuclear materials. These 13 "licensees" operate 15 distinct facilities. These companies and licensees will be directly affected by any government actions resulting from the findings and recommendations of the task force.

Task Force Approach

The action plan developed by the task force was derived from two sources of site-specific safeguards information: one source was the safeguards site review and inspection activity conducted during the spring of 1976, to assess the adequacy of current safeguards for SSNM against specified threats formulated

TABLE I-1

INDUSTRY PARTICIPANTS

Babcock and Wilcox Company

Battelle Memorial Institute

Exxon Nuclear Company, Inc.

General Atomic Company

General Electric Company

Kerr McGee Nuclear Corporation

Nuclear Fuel Services, Inc.

Rockwell International Corporation
(Atomics International Division)

Texas Instruments, Inc.

United Nuclear Corporation

U.S. Nuclear, Inc.

Westinghouse Electric Corporation

for planning purposes. These reviews indicated that the licensees were generally in compliance with NRC safeguards regulations but indicated that improvements were needed at each facility to achieve the levels of material control and physical protection desired by both ERDA and NRC. The other source was site-specific plans prepared by each of the licensees outlining the additional safeguards measures they would propose in support of the task force objective. These industry plans were derived from the licensees' perceptions of how their current safeguards could be improved as well as from performance criteria provided by the task force for this planning activity.

The task force selectively used these site reviews and industry plans as the basis for identifying both generic and site-specific safeguards measures that could meet performance criteria. The steps to implement these measures were organized into a time-phased plan of action. The measures were also examined for their implications in industry, ERDA, and NRC activities.

In formulating an action plan based upon the site review and industry proposals, the following questions emerged as basic issues to be resolved in accomplishing the purposes of the task force.

1. Are we satisfied with the current level of safeguards protection for the foreseeable future?
2. If not, what level of threat should safeguards protect against?
3. How soon should that level of protection be attained?

The first question is pivotal: the safeguards posture implicit under present regulations is intended to counter the diversion or theft of strategic special

nuclear material by one insider or an external group of two or three individuals armed with handguns or shotguns.* If the current posture were deemed insufficient because the defined threat level were judged as being too low, the next steps in safeguards improvements may well be significant changes for both government and industry.

It is important to note that the task force was charged with developing an action plan to assure confident control and protection of SSNM. Obviously there are no absolute means for assuring the security of nuclear materials so long as they exist and are used anywhere in the world. While the proposed action plan cannot guarantee the security of nuclear materials, it can provide for safeguards capabilities that should give high confidence in our ability to prevent the theft or diversion of SSNM.

*Protection against an internal threat of one is implied in 10 CFR Part 73. Regulatory Guide 5.43 states that security forces should be capable of: preventing actions by one or two armed individuals or a group of unarmed people; delaying an armed group of up to squad size to allow response by law enforcement authorities; and defending itself in the event of a well planned attack executed in a disciplined and organized manner to allow communicating with law enforcement authorities.

II. SAFEGUARDS SITE REVIEWS

In January 1976, the NRC initiated a comprehensive review of the current safeguards at licensed facilities handling strategic special nuclear material (SSNM). The primary purpose of the review was to evaluate each of the licensee's safeguards capabilities to protect against the theft of nuclear materials in suitable quantity and form for the illicit manufacture of nuclear explosives.

Onsite visits to 13 licensees (involving 15 distinct facilities) were conducted to provide a direct and detailed assessment of physical protection and material control capabilities. These capabilities were examined with respect to an assumed internal threat of one employee occupying any position or an assumed external threat comprised of three well-armed (legally obtainable weapons), well-trained individuals, including the possibilities of inside knowledge or assistance of one insider. The facilities involved, the dates of the onsite visits, and the composition of the review teams are displayed in Table II-1.

Evaluation of each licensee's capabilities was made on the basis of effectiveness against an assumed threat rather than technical compliance with present safeguards regulations. A set of performance criteria was developed to insure that the evaluations were as comprehensive and consistent as possible.

The results of the reviews indicate that improvements in physical protection and material control (containment measures and access controls as opposed to material accountability) would be needed at each facility in order

TABLE II-1
SAFEGUARDS SITE VISITS

LICENSEE	DATES OF REVIEW 1976	TEAM COMPOSITION
Nuclear Fuel Services (Erwin)	1/13 - 1/15	NRC Material Control Task Group
	2/ 2 - 2/ 3	NRC Material Control Task Group
	2/18 - 2/20	NRC Physical Security Team
Babcock and Wilcox NMD (Apollo, Parks Township)	1/27 - 1/29	NRC Material Control Task Group
	4/ 4 - 4/ 9	NRC Physical Security Team NRC Material Control Team ERDA Team
U. S. Nuclear (Oak Ridge)	2/ 8 - 2/11	NRC Physical Security Team
	2/18 - 2/20	NRC Material Control Team
General Atomic (San Diego)	2/11 - 2/13	NRC Physical Security Team
	3/ 1 - 3/ 3	NRC Material Control Team
Atomics International (Canoga Park, Chatsworth)	2/14 - 2/20	NRC Physical Security Team
	2/25 - 2/27	NRC Material Control Team
Texas Instruments (Attleboro)	2/24 - 2/27	NRC Physical Security Team
	3/ 8 - 3/10	NRC Material Control Team
United Nuclear (Uncasville)	3/ 2 - 3/ 5	NRC Physical Security Team
	3/ 9 - 3/11	NRC Material Control Team ERDA Participant
Babcock and Wilcox NNFD (Lynchburg)	3/16 - 3/19	NRC Physical Security Team NRC Material Control Team ERDA Participant
General Electric (Vallecitos)	3/21 - 3/24	NRC Physical Security Team NRC Material Control Team
Exxon Nuclear (Richland	3/25 - 3/27	NRC Physical Security Team NRC Material Control Team
Battelle Columbus Labs (Columbus)	3/13 - 4/15	NRC Physical Security Team NRC Material Control Team ERDA Team
United Nuclear (Wood River)	4/20 - 4/23	NRC Physical Security Team NRC Material Control Team ERDA Participant
Westinghouse (Cheswick)	4/21 - 4/23	NRC Physical Security Team NRC Material Control Team ERDA Participant

to counter the threat levels defined for the evaluation. Capabilities found inadequate were: control of access to SSNM, positive containment of SSNM, and protection of SSNM from theft by means of an external assault.

The review generally found licensees to have comprehensive safeguards systems in place, but the evaluations of system effectiveness highlighted the existence of inadequacies in their capabilities to counter the threat levels defined for this review. The evaluations also revealed significant variations in safeguards capabilities. Consequently, there were marked differences from one licensee to the next with regard to their overall ability to counter the specified threats.

The most prevalent deficiencies were those related to the control of access to SSNM (both stored and in process), exit search procedures, and the adequacy of response by onsite and offsite forces. The review teams indicated that short-term fixes could correct most of the weaknesses at each facility. Although some of the improvements needed to improve safeguards capabilities involve structural changes, most could be resolved by procedural means.

Actions to correct the safeguards inadequacies are being accomplished within the existing regulatory framework. Matters that cannot be resolved through negotiation are being resolved by the imposition of additional or more specific license conditions on a case basis.

Based on these actions and subsequent reviews of the 15 facilities involved as of the end of May 1976, two facilities have safeguards that were judged vulnerable to both the external threat of three and internal threat of

one. Four facilities were judged inadequate against the postulated external threat and one was judged vulnerable to internal material diversion by one employee. The remaining inadequacies at these seven facilities are being improved by a combination of voluntary actions on the part of the licensees and government directed actions. These improvements are planned for completion by August 1976.

ERDA Facilities Comparative Review

A joint ERDA-NRC team visited three representative ERDA facilities to evaluate the effectiveness of safeguards programs and to provide a reference for assuring the parity of safeguards between NRC-licensed and ERDA license-exempt facilities. The threat criteria used to make these evaluations were the same as those used in evaluating the licensed facilities: an assumed external threat of an armed group of three, including the possibility of inside knowledge or assistance, or an assumed internal threat of one individual occupying any position.

Conclusions were:

1. Present capabilities are more than adequate against an unassisted external threat assumed in this review.
2. The facilities could not, with a high degree of assurance, protect against an external force in possession of inside knowledge or assistance and operating in a covert manner because of inadequate, marginally effective detection aids.

3. One facility could not, with a high degree of assurance, prevent the diversion of significant quantities of SSNM by an insider. Improvements were needed at all three facilities in the techniques used to prevent the diversion of significant quantities of SSNM.

A number of actions which would correct the identified inadequacies were already scheduled and funded in present and succeeding annual programs. As an interim measure, the noted deficiencies were corrected by short-term actions and each of the facilities is presently judged to have the capability to effectively counter the external or internal threat levels used as review criteria.

III. THREAT CONSIDERATIONS

The present regulatory approach permits some ambiguity about the level of threat against which safeguards are expected to prevent the theft or diversion of SSNM. The threat is only implied in the specific systems and procedures delineated in regulations, guides, and license conditions. Without defining the adversary that might use or threaten to use SSNM, 10 CFR Part 73 prescribes physical security measures in terms of specific actions and procedures that the licensee must follow. Although not stated explicitly, the safeguards provisions of 10 CFR Part 73 are clearly compatible with the present regulatory posture of protecting SSNM against diversion of one person who has access to SSNM or armed robbery by a group of two or three with light armament (i.e., legally obtainable weapons such as handguns, rifles, or shotguns).

The specification of threat levels is a central aspect of continuing efforts to insure the adequacy of safeguards. Early safeguards for privately held SSNM reflected the typical industrial security afforded to valuable materials. With the advent of terrorist acts to extort subnational goals or large sums of money, security measures were increased to protect SSNM from theft or diversion to prevent its illicit use. Recent social changes and the increasing propensity of individuals and groups to resort to violence to obtain their goals indicate the dynamic nature of safeguards and the problem of determining what level of safeguards is adequate.

Many efforts have been made to determine what kinds of threats could be directed against the nuclear industry. These have included numerous studies and discussions with law enforcement, research, and intelligence organizations. Despite these efforts, the threat remains an inherently indeterminate question. Yet, safeguards systems must be planned, designed, built, and operated in the face of these uncertainties. Decisions on levels of protection are further complicated because the threat is a multidimensional entity, which cannot easily be described or reduced to simple decision variables.

Threat Information

There are three basic sources of threat information: historical data, current intelligence, and speculation. While there is considerable worldwide historical background on criminal and terrorist activities, the relevance of these data to threats against the U.S. nuclear industry is problematical. There is little basis for confidence that one can project the past as the future. The primary usefulness of historical data is that it may provide insights into the general nature of threats and illuminate situations which may be analogous to those in the nuclear industry.

Current intelligence is an obvious source to be exploited, but there is little verified data available to identify specific threat groups and their intentions. Law enforcement agencies believe that the larger the group attempting to plan and organize an assault on a nuclear facility, the greater the probability their activities would be detected and some advanced warning would be provided. However, it is difficult to quantify that detection threshold in the absence of specifics.

Speculation, on the other hand, is common. Basing safeguards upon speculative threats poses several problems. Such threat definitions are highly subjective and tend to be boundless; it is virtually impossible to define the demarcation between credible and incredible threats.

The use of "maximum credible threat" is frequently suggested to overcome the difficulties (or compensate for the uncertainties) arising from lack of specific information on the threat. This concept requires judgments on two counts, both of which are necessarily subjective. First, there is the problem of where to establish the boundary between what is credible and what is incredible as a threat. Many people would agree that a very small threat (two or three individuals) is credible and many would agree that some very large threat (40 or 50 individuals) is incredible. It is difficult, if not impossible, to obtain a consensus at many points in between. Second, there is the problem of estimating the likelihood of such a threat materializing (if it can be defined at all). Furthermore, the "maximum credible" threat is not particularly useful as a decisionmaking concept because severe civil disorders and states of war, while quite credible, are not a rational basis for designing routine security for a regulated commercial industry. At some point in the spectrum of what is considered "credible," industrial security by means of regulation becomes implausible.

Threat Alternatives

Historical data indicate that there is a wide spectrum of motivations for theft and terrorism. However, there is no evidence available to indicate

any current threat of theft or diversion of SSNM. Current information does not identify any persons or groups as posing an apparent threat to steal SSNM, nor has any black market been detected that would provide motivation for theft of SSNM. The most plausible incentives for theft or diversion of SSNM appear to be the possession of nuclear materials for the purpose of extortion, ransom, or public attention.

The threat of theft or diversion could come either from within a facility or from an external group. The internal threat could be a single insider or a conspiracy of two or more working surreptitiously to defeat the safeguards system.

To define alternative levels of threat, the task force described the external threat by the following characteristics: mode of operations, arms and equipment.

Adversary modes of operation could be characterized as either "professional armed robbery" or "determined violent assault." The external threat against which the detailed systems and procedural requirements of 10 CFR Part 73 provide protection can be loosely described as a "professional armed robbery." This threat was previously defined as two or three persons armed with legally obtainable "light" weapons, such as pistols, rifles, and shotguns. Their skills would approximate those of a professional robber and while they might be willing to take the lives of others to achieve a theft or to prevent their own capture, they would more likely prefer to use stealth or merely threaten to kill. They would be willing to accept some personal risk, but would

probably abandon their attack if confronted with serious threats to their own lives.

"Determined violent assaults" on the other hand, would be substantially more severe than "professional armed robberies" in terms of armament and motivation. They might nominally consist of armed terrorist-type groups. They would have few inhibitions about killing others to achieve a theft, and they would probably be willing to risk their own lives to do so; they would probably abandon their attack only if defeat were imminent. In the extreme, a "determined violent assault" could consist of fanatics, with similar armament, who would have no inhibitions whatsoever about killing and would continue their attack to the last man. For these violent threats, the discipline, motivation, and training would be beyond those of a professional robber, and might approximate those resulting from commando-type training.

The availability of sophisticated armaments to individuals or criminal groups is changing rapidly. Automatic rifles and plastic explosives are now widely available. Arms could range from legally obtainable weapons such as handguns, shotguns, and rifles up to light automatic rifles (M-16s) and heavy calibre machine guns (M-60s). Modern, high-technology weapons, such as wire-guided and heat-seeking missiles, recoilless cannons, helicopters, etc., cannot be excluded as possibilities even though unlikely based upon current evidence.

The size of the group has the potential for as much variability as the other characteristics. Historical data on the numbers of persons involved in

groups committing robberies, assaults, and acts of terrorism show that small groups predominate. Larger groups account for only a few percent of the cases, although there are isolated instances of very large groups. The relevance of this historical data to the future or to threats involving the theft of SSNM is problematical except as a point of departure.*

In the absence of specific evidence of threats, safeguards planning must necessarily be based upon hypotheses of motivations and estimates of capabilities. The primary determinants of threat capabilities for theft are the numbers of persons involved, their access to positions of trust with respect to SSNM, the availability of arms or special equipment that might facilitate a theft, and their willingness to sacrifice lives to achieve success.

Threat Recommendation

Based on the historical data, currently available intelligence, and extensive deliberations, the task force has developed a threat definition sufficiently broad for decisionmaking, yet with enough detail for safeguards design.

With respect to internal threats, it is recognized that any employee could become disgruntled, emotionally disturbed, involved in a subversive group or financially troubled at anytime and consequently misuse his access

*A study by the BDM Corporation of 4478 incidents including armed attack, arson, bombing, kidnapping, and hijacking identified 1271 cases in which the number of perpetrators was known. Of the cases in which group size was reported, 58% of the incidents involved a single person; and those involving groups of more than six persons accounted for 2.5%. Groups with more than ten attackers were recorded in less than 1% of the incidents. Similar studies by others produce roughly the equivalent results; however, there are so many qualifications that might be placed on the distribution of group size and types of incidents examined that such studies provide only a point of departure for considering the possible size of potential threats.

to SSNM. Therefore, the safeguards system must protect with high confidence against the diversion or theft of SSNM by any single insider, regardless of position or clearance.

Safeguards planning must also address the possible conspiracy of insiders, since there are many examples of employees working together to steal or embezzle from their employers. The possibility of insiders participating in or instigating the theft of nuclear materials is considered by many to be more likely than an armed assault by outsiders. Thefts in commerce frequently involve insiders, and internal conspiracies are not uncommon in the hijacking or diversion of commercial freight.

Systems and procedures can be installed within industrial facilities to protect against internal conspiracies, but they probably will require additional people, interfere with process operations, and necessitate physical rearrangements or additional security equipments in some plants. It may be operationally impractical to design such measures to be completely effective against conspiracies involving key management and security personnel. Thus, reliance upon personnel clearances may be necessary for key personnel. It is generally accepted that clearances based on full-field background investigations substantially reduce the likelihood of malevolent conspiracies. This principle is a basis for protecting many national resources, including nuclear weapons.

Nevertheless, prudent safeguards system design would make maximum use of technology and procedures to prevent conspiracy wherever practicable, even where personnel have been cleared. In any event, clearances should not be

deemed adequate insurance against the theft of SSNM by any single insider, regardless of position or trust. Thus, safeguards should protect with high confidence against conspiracies involving insiders (except where possible conspirators have clearances based on full-field background investigations).

With respect to external threats, safeguards should be able to protect with high confidence against "determined violent assaults." These threats would be substantially greater than "professional armed robberies" in terms of adversary numbers, armament, and motivation. They would consist of armed terrorist-type groups. Such safeguards should also include the capability to protect against fanatics who would have no inhibitions whatsoever about killing and would continue their attack to the last man. The recommendations on adversary numbers reflect a belief that willingness to risk and inflict violence are less likely as the number of adversaries increases. Also, the capability to protect SSNM with high confidence against determined violent assaults by small groups is believed to retain a substantial capability in the unlikely event of an assault by even larger groups (whose operations would challenge the existence of civil order).

In the absence of specific threats to the nuclear fuel industry, any decision as to what levels of protection are adequate is inherently judgmental. While the task force believes that protection against conspiracies or determined violent assaults provide a reasonable level of protection, there are persons who would be satisfied with less security as well as those who would insist upon more. If a decision is made to accept the protection levels

recommended by the task force, some might urge that this protection be provided immediately by emergency means, such as the use of federal forces. The task force believes, as a matter of judgment, that safeguards should be upgraded expeditiously. In the absence of specific threats to the industry, the task force does not consider emergency measures are warranted; however, interim measures may be warranted to increase safeguards capabilities during the period required to implement a complete upgrading program.

IV. PLANNING REQUIREMENTS

Generalized performance requirements for the control and protection of SSNM were defined by the task force for coordinated planning with industry, ERDA, and NRC. These requirements were used by the licensees as guidance in preparing proposed plans for improving the safeguards at their facilities.

The planning requirements included, first, a description of the basic functional capabilities deemed essential to assuring the control and protection of SSNM against theft or diversion and, second, a definition of the required degree of assurance against specified adversaries.

Basic Capabilities

The basic functional capabilities defined by the task force were intended to assure the protection of SSNM against theft or diversion. They supplement the detailed systems and procedural requirements of 10 CFR Part 73 for the physical security of special nuclear materials. Five basic capabilities to assure the physical security of SSNM were identified. Two of these capabilities relate to the control of access to SSNM, two relate to the containment of SSNM, and the last relates to protection against external assaults. The basic capabilities are those that will assure:

1. admission of only authorized personnel and materials into SSNM access areas,
2. timely detection and effective responses to unauthorized conditions of access to SSNM or unauthorized activities within SSNM access areas,

3. removal of only authorized and confirmed materials from SSNM access areas,
4. timely detection and effective responses to breaches in the containment of SSNM, and
5. timely detection and effective engagement of intruders penetrating protected areas.

The following descriptions are intended to amplify and give examples of the basic capabilities.

Capability 1: Admission of only authorized personnel and materials into SSNM access areas.

Systems and procedures should verify the identity of individuals entering an SSNM access area and exclude unauthorized individuals from these areas. Badge and identification systems can be used to verify the identity of unauthorized persons. Barriers can be used to restrict unauthorized access. One intent of the statement of capability is to exclude from access areas any materials that could be used to advance the theft of SSNM, except when such materials would be required in an access area for legitimate and authorized purposes. Appropriate searches or other methods could be used to provide assurance that only authorized materials enter in packages, in vehicles, or on the person of individuals entering.

Capability 2: Timely detection and effective responses to unauthorized conditions of access to SSNM or unauthorized activities within SSNM access areas.

Safeguards should identify and deal with any conditions in a facility that might permit unauthorized persons to have access to and steal SSNM. Unauthorized access could include having employees in areas where they are not permitted, having unauthorized persons handling SSNM without a desired level of surveillance, or other similar situations. Detection of unauthorized conditions of access might result from the use of various alarm systems or surveillance techniques. Alarm systems such as motion detectors provide one means of detection, while surveillance techniques such as the use of guard patrols, closed circuit television coverage of illuminated protected areas, and two-man rule are also candidates for detecting unauthorized access. Tests can be used to demonstrate the effectiveness of sensor-type systems.

Capability 3: Removal of only authorized and confirmed materials from SSNM access areas.

All SSNM should be kept in its proper locations within access areas except when removal is required for some legitimate purpose; and when required, some means should be provided to confirm that the material actually leaving is that which is supposed to leave.

This capability can be achieved by securing a known quantity of SSNM in a given location to prevent its removal. Barriers, containers, tamper-safing, storage of material not in process, and the use of pressure sensitive alarms to detect removal are several examples of means of securing SSNM. The capability also might involve detection of an attempted unauthorized removal of SSNM by using search procedures. In either case, a potential diverter

should not be able to get SSNM outside an approved access area. If used, search procedures should work if the diverter attempts to conceal the material on his person or in some other material or container leaving the area, or if he attempts to shield the material from discovery by SSNM detectors.

Capability 4: Timely detection and effective responses to breaches in the containment of SSNM.

Much of the protection afforded SSNM is likely to be provided by barriers and containers. This capability requires that detection and appropriate response be taken when the security of the SSNM is threatened by one or more of these protective containment structures being breached. Examples of containment breaches include uncovered ventilation ducts which could permit passage of people or material, breaking of a tamper seal on an emergency exit or material container, a hole in the wall of a vault, an accidental or intentional break in a pipe, siphon from a liquid storage container, or other similar conditions.

Detection methods are likely to be similar to those employed to detect unauthorized access, and might include alarms, surveillance, guard patrols, and inspection of containment structures on a regular basis. If a breach of containment is detected, the appropriate response should correct the situation to the extent that an attempted theft would be prevented or discovered in time to prevent the loss of SSNM.

Capability 5: Timely detection and effective engagement of intruders penetrating protected areas.

An expected sequence of response to an external assault might consist of attempted intrusions being detected, assessed, and delayed by means immediately available until an effective response can be mustered. A number of diverse capabilities could be traded-off against each other to achieve this capability. For example, with sufficiently formidable barriers, it might be possible to have delays which would permit significant reductions in on-site guard forces. Response forces from both on-site and off-site can be used, but their arrival should be timely and effective enough that they would be expected to prevail against the adversary group. Communications of various types can be used to summon response forces, as long as the capability can be shown to exist in depth.

Factors that might be considered in evaluating the expected effectiveness of response forces include their motivation, training, physical condition, armament, numbers, and protection afforded by defense positions. Defensive positions offer potential advantages to the response forces and, if present, can reduce the total numbers of guards required, help provide additional delay, and compensate to some degree for disadvantages in armament or other factors.

Performance Criteria

The safeguard systems designed to provide these capabilities should be expected with high confidence to thwart a theft of SSNM. A theft should be considered successful when the adversary has taken possession of the SSNM free from any immediate interceding actions (engagement or hot pursuit) of the response forces.

The nuclear materials of greatest concern are those which could be used for nuclear explosives. Protection of SSNM should preclude the theft of 2000 grams or more of plutonium or uranium-233, or 5000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope) in a single theft or continuing series of thefts within a 12 month period. These quantities are judged to be substantially less than that required for the illicit manufacture of a nuclear explosive.

V. DESCRIPTION OF UPGRADED SAFEGUARDS

Each of the licensees was asked to submit a plan to the task force indicating the improvements they considered necessary to meet the performance criteria, as well as the associated costs and time for implementation. This section summarizes the plans submitted by industry and describes a composite view of the safeguards that would result from a decision to protect SSNM against the specified threats. The plans are not a consistent set, since they were prepared from two different specifications for a design threat. Most of the licensees based their plans on an initial design threat definition derived from existing rules and guides; however, some of the licensees chose to work with a later definition of internal conspiracy and a small group of external violent attackers. Moreover, the plans were completed on a very short time schedule and represent no more than preliminary thoughts and rough estimates of how the industry might respond to the performance criteria.

Most of the licensees indicate that they would meet the criteria primarily by providing both delay mechanisms (barriers and guard posts) and additional security personnel. While several of the licensees emphasized delay mechanisms, none of them elected to satisfy the criteria with manpower-intensive techniques.

The physical improvements most often appearing in the industry plans are the following:

1. Additional or modified guard posts. These include such provisions as hardening or upgrading existing posts by providing bulletproof windows or adding other protecting equipment.

2. Addition of fences or barriers. Nearly all of the licensees would add to their existing barrier systems to provide delay against intruders and provide isolation of perimeter areas to be kept under surveillance. The most common improvement is the addition or hardening of perimeter barriers. Methods of upgrading fence lines include the installation of vehicle gates and barriers and the addition of concertina wire barriers behind fences.
3. Modification or consolidation of SSNM process areas. Most of the licensees would modify their plants to make the physical protection of SSNM easier. These changes would generally involve isolating sensitive areas and reducing the size of these areas that would require extraordinary protection. Several licensees would move non-process activities, such as lunch rooms, out of SSNM access areas. Others indicate that they would construct additional vaults, change rooms, or emergency bunkers.
4. Improved surveillance. Enhanced surveillance capabilities are common to nearly all licensee plans. The use of closed circuit television and other surveillance techniques, including additional guard towers affording surveillance and control of large areas of a facility, is seen as a means of protecting against both internal and external threats. Additional surveillance of plant perimeters would provide external threat detection and assessment capability, while upgraded surveillance of SSNM access areas and entry/exit points would provide additional protection against internal threats. Upgraded exterior lighting would be employed at several facilities.

5. Improved entrance and exit procedures and equipment. These measures are regarded by the licensees as fundamental to achieving the personnel access and material containment objectives. While some licensees would further restrict the number of personnel granted access or improved personnel search procedures (including random search), others would design new systems or procure new equipment for control of entry and exit. Among the design alternatives are computerized identification and admittance systems, relocation or expansion of search areas, and the prohibition of personal articles in SSNM access areas (with lockers provided outside the areas). Equipment procurement would include better SSNM and metal detectors, X-ray machines for package search, and assay equipment to measure SSNM content.
6. Augmented detection and alarm systems. Most licensees would upgrade early detection and alarm systems in association with external barriers. One licensee would use continuous perimeter patrols to enhance detection, while another would create and patrol a wide isolation zone. Motion detectors and alarms would also be employed in SSNM access areas to protect sensitive process areas when unoccupied.
7. Addition of response forces. Nearly all of the licensees believe that they would have to add to their on-site response forces to cope with the external threat. Several licensees propose to have ten guards on site at all times. Some believe that it is important to have a dedicated response force in addition to those guards performing ancillary functions such as access control, escort, and surveillance. Several indicate that they would prefer

company guards over contract guards so as to maintain greater control over qualifications and training and to better assure the appropriateness of responses.

Other improvements appearing less frequently in the plans include the upgrading of emergency power and communications systems. Several unique approaches were also proposed. One approach requiring additional developmental effort would delay intruders by a combination of vehicle barriers around the facility, flooding the process areas with nonirritant smoke to impair vision, covering the facility floor with the slippery liquids used for riot control, and coating sensitive SSNM containers with quick-hardening plastic foaming agents in the event of armed attack.

About half of the licensee plans indicate improvements that could be characterized as "major" changes from their current safeguards approaches, while an equal number indicate "moderate" changes. Two licensee plans propose only "minor" changes, while another claims their current safeguards meet the criteria.

In summary, a substantial number of changes would be required by the licensees to bring their safeguards performance up to the level required to meet the threats of an internal conspiracy or a determined violent assault. There appear to be no technological problems that would prevent any licensee from adequately meeting these levels of threat; however, there may be some formidable psychological obstacles. There is considerable reluctance expressed by industry to accept responsibility for protecting SSNM against determined

violent assaults. This reluctance stems from industry beliefs that (1) this level of threat should be a federal responsibility, (2) the necessary levels of defense would be damaging to company images, (3) the government should first resolve several issues which are seen as impediments, and (4) the future of safeguards requirements offers too many uncertainties. Several licensees profess to be sufficiently concerned to consider withdrawing from activities involving SSNM.

If a decision is made to upgrade safeguards, preparing to meet the internal conspiracy may require organizational or line-of-authority changes which would prevent two individuals from subverting the safeguards system by issuing new directions to the guard force or varying other procedures. As a general approach to meet the internal conspiracy, most licensees would severely restrict access to material and provide surveillance of those who have access. Many of the licensees would modify or consolidate process areas to facilitate access restrictions. The procedures used to protect against conspiracies would generally be expected to slow production. Closed circuit television (CCTV) would be widely used for maintaining surveillance over entrance, exit, and operations where people have direct access to SSNM. It would be necessary to provide personnel security clearances for guards and other key people.

Nuclear facilities configured to defend effectively against determined violent assaults would differ considerably from current facilities. These differences would involve both the security forces and physical characteristics of the facilities. Whereas current facilities typically have on duty at any

given time fewer than six lightly armed guards, a guard force configured to defend against determined violent assaults might consist of as many as 10 to 12 well-armed and protected guards. Some companies would employ dedicated response forces, which would not be encumbered with visitor control, search, or other similar duties.

The physical characteristics of nuclear facilities would also be likely to change significantly if configured against determined violent assaults. Most licensees would develop defenses in depth, possibly including as many as three external fences, vehicle barriers, hardened guard posts, watch towers, or other defended positions, and additional detection and alarm systems. In summary, a plant configured for the larger threats would be expected to present an external appearance dominated by multiple security barriers, detection and surveillance equipment, and hardened defensive positions for guards.

Half of the 14 licensees estimate individual capital costs of $0.5M or less, while another 5 show capital costs in the range of $0.7 to $1.5M. Annual operating costs are less than $0.5M for all but four licensees. The cost estimates included in the industry plans are preliminary and were intended to provide only a first order estimate of the added costs to upgrade safeguards. The plans were completed to meet the schedule of the task force and there was insufficient time to do more than make rough approximations. In some cases the licensees believed the estimates were within a factor of two of what should be expected as a final cost. In other cases the estimates were considered accurate within plus or minus ten percent because the planning detail was

sufficient to make better cost estimates. The task force estimates that the total added costs would be somewhat higher than the licensee estimates to effect these changes for the 14 facilities. The total would more likely be about $20-25M for capital expenses (30 to 50 percent for construction and the balance for equipment) and between $10-15M for annual operating costs (about 80 percent for guard and other salaries); these estimates are subject to substantial revision with more detailed planning to design systems to meet the upgraded performance requirements. The variations in cost from one facility to another would also be substantial, perhaps by a factor of three.

The licensees estimated that it would require from 6 to 24 months from a starting date to complete the upgrading of the facilities. The construction of fences and guard posts could be completed within several months. The construction involving modification of buildings and process areas and the installation of surveillance and detection equipment would generally require 12-18 months.

The 14 plans submitted by industry were reviewed by members of the technical staffs of ERDA, Sandia Laboratories, and Brookhaven Laboratories to determine whether or not the plans, if implemented, would be capable of meeting the performance criteria. While noting that the plans were not in sufficient detail to permit an in-depth analysis of the proposed safeguards, this technical review indicated that about two-thirds of the plans could reasonably be expected to protect against assaults by a small group of attackers with insider assistance. Licensee capabilities against internal conspiracy threats could

not be determined in this technical review because most license plans considered only single insider threats. The review team noted that the plans, including the cost data, are adequate for preliminary planning but that additional detailed planning would be required. They also confirmed that the measures necessary to protect against the higher threats could be put in place only through mid- or long-term efforts.

In summary, the plans represent a conscientious effort on the part of the licensees to identify improvements necessary to meet the performance criteria. Most of the plans indicate measures which would be expected to protect adequately against a small group of attackers having inside assistance. Although there is considerable variance in the aggregate of licensee plans, the safeguards described by a composite view of the responses are distinctly beyond those required by existing regulations.

VI. MAJOR DECISION ISSUES

The upgrading of physical security at licensed fuel cycle facilities will require the resolution of two kinds of issues. The first type, program definition issues, are those matters which must be resolved before the licensees can (or will) proceed in developing the design for an upgraded system. These issues include definition of the threat, the schedule or goal for completing the upgrade, and whether the upgrade program objectives and performance requirements will be disclosed at the outset. The second type, implementation issues, concern the financial arrangements for meeting the costs of upgraded safeguards and regulatory means for achieving the upgraded posture.

Threat

Present regulations do not explicitly define the threats to SSNM nor specify the levels of performance that licensees are expected to meet in order to protect SSNM. The licensees' posture for protecting SSNM, as derived from present regulations and reflected in the site assessments, generally provide reasonable protection against single insiders or groups of about three attackers. If the licensees are required to substantially increase their levels of protection, and if the adequacy of their safeguards is to be measured in terms of performance, then they need to be provided information on threats as a basis for their planning. Without a well defined and approved threat, the licensees have no logical basis for determining the nature and extent of their safeguards systems.

A design basis threat is required for the rational design of safeguards systems and procedures and to evaluate their effectiveness. The importance of threat specifications for safeguards design and evaluation would seem to increase with the severity of the threat since the necessary additional measures are increasingly associated with the threat (as opposed to basic security provisions independent of threat levels). As discussed in Chapter III, determining a design threat level is basically a matter of judgment. Eventually ERDA and NRC must define an internal and external reference threat level to provide a basis for the design and evaluation of safeguards systems that will assure confident control and protection of SSNM.

Schedule

After determining the threat and corresponding level of safeguards, the next issue is how quickly should that level of safeguards be attained. For example: if the internal threat is defined as a conspiracy and the external threat is defined as a determined violent assault, should safeguards be immediately postured to protect against that threat, or is that goal to be achieved sometime in the future, say two or four years hence? Resolution of the schedule rests in part on judgment of the urgency in meeting the defined threat.

The task force estimated that routine regulatory procedures could require up to two years just to address and resolve policy questions that directly affect safeguards system design. Many of the policy questions require preliminary study and analyses to develop a basis for a reasoned position. Such

studies can require from a few weeks to several months. Preparation and coordination of important policy decision papers typically involve months rather than weeks. Publishing a proposed rule for comment and possible hearings can add from three to six months to the process. If the proposed actions are contested, extensive delays could result. The nature of the policy questions indicates that a two-year estimate for resolving such questions may be optimistic. These policy questions include:

Guard Force Weapons and Authority - Preparing a safeguards plan to protect a facility against a determined violent assault raises the question as to what armament the guard force may use. The use of special weapons such as automatic rifles or machine guns could influence the numbers of guards, the location and construction (hardening) of guard posts, control and communication capabilities, and possibly different locations and construction of barriers.

The use of automatic weapons is to some extent restricted by both federal and state laws. The contribution of these weapons to guard capabilities should be determined so that a factual basis can be developed for determining whether or not to seek relief for the licensees from such restrictions. Such relief might help resolve the philosophical problem that arises from directing the licensees to defend SSNM against attack by a determined violent group that could be expected to have automatic rifles while denying the licensees the option of using equivalent weapons.

As an alternative, the use of semi-automatic rifles (e.g., AR-15s), could be authorized or directed without enabling legislation. These weapons would provide a substantial increase in the firepower of the on-site response force.

Plant guard forces are an essential element in the physical protection of nuclear facilities, because it is they who ultimately determine the outcome of any attempted theft of SSNM. For this reason, it is imperative that there be no doubts as to the authority of guards to act in the defense of SSNM.

Several other issues related to guard force capability and involving the use of force need to be clarified or resolved because the outcome of those decisions affect cost-effectiveness design tradeoffs. According to the NRC legal staff, present laws provide adequate authority for guards to use deadly force to prevent death or serious injury and to repel armed attacks. The most troublesome area in which the use of deadly force is not clearly permitted by law is in preventing escape of persons stealing SSNM. Since the use of deadly force in the protection of SSNM may not be legally separated from existing homicide laws, this problem could be alleviated by legislation authorizing special use of force to protect SSNM.

The arrest authority of guards is the same as that of other private persons. Generally, a guard can arrest for any offense committed in his presence, but can only use the minimum force necessary to effect the arrest. Under present laws, trespass on a nuclear facility may not be an arrestable

offense unless the person has felonious intent. Several possible legislative actions are available: (1) making trespass on a nuclear facility a criminal act, per se, (2) enlarging the arrest authority of guards, or (3) extending the trespass provisions of the Atomic Energy Act of 1954 to include the private property of licensees.

The unresolved questions that presently exist in the minds of the licensees about the limits in the use of deadly force by their guards become a greater problem in the context of defending against determined violent assaults. It is important that the federal government, in conjunction with local legal authorities, clarify these issues for the licensees so that guard authority is clearly understood. A legislative change in legal authority would necessarily be a long-term action. While some changes in legal authority of licensee guards would undoubtedly improve their cost effectiveness, such changes are not now seen as essential to an adequate safeguards posture.

Guard Selection and Training - The requirement to defend against a determined violent assault would call for a guard or response force consisting mostly of physically-fit individuals who are trained and emotionally prepared for combative action to protect themselves, their facility, their fellow employees, and the nuclear materials entrusted to them for protection. The need for physically fit, trained, and emotionally prepared individuals for guard duty could be met by a federal program to establish qualifications, testing, and licensing of guards, although the latter would require a legislative action.

In addition to physical fitness and abilities, the selection of guards for employment should be based upon a thorough investigation of their background, moral character, and psychological stability. The authority to conduct an industrial security clearance program and other pre-employment screening is available but staff and Commission action is required to prepare and issue the necessary rules.

Technical Assistance - In 1975, the National Security Council approved limited ERDA assistance in the form of research and development of a generic nature to help fuel cycle licensees comply with safeguards regulatory requirements. Accordingly, ERDA is developing design guides for safeguards, plans to demonstrate systems in the light water reactor fuel cycle, and is testing commercially available safeguards equipment. The hardware performance specifications being developed as a product of these efforts will be generally available to licensees. The performance and limitations of commercially available equipment and systems tested by Sandia Laboratories and by Los Alamos Scientific Laboratory will be made available to the manufacturer and as needed by licensees to design safeguards systems and select components for their installation.

Historically, ERDA/NRC staff and laboratories have responded to casual information requests from facility operators for readily available information. Consulting on safeguards system design and selecting types of equipment may, in addition, include participating at technical meetings to help develop or evaluate plans for specific facilities. These services

are available from ERDA laboratories to the extent needed to plan for implementation; they are also available during and after implementation to the extent that the requested services do not interfere with higher priority safeguards missions of the laboratories. The experience gained by the ERDA laboratory staff is a consideration in specific decisions to provide such consulting services.

Government-owned safeguards equipment being held for contingency use may be provided to commercial facilities for safeguarding nuclear materials held or used for government purposes. This would consist primarily of equipment for physical protection under agreements that would not hold the government responsible for maintenance, repair, or liabilities resulting from equipment malfunction.

Authority exists for ERDA and NRC to provide clearances and classified information on a need-to-know basis. An administrative procedure is needed to establish clearances on a need-to-know basis to provide classified information for use in the design of safeguards systems.

Government assistance can assure the uniform effectiveness of guards for nuclear facilities. Guard effectiveness depends in large measure on the nature and quality of specialized training. Large contract guard companies may be able to provide such training with minimum government assistance in designing the curriculum. Most nuclear facility operators indicated their preference for using company employees as guards in planning safeguards systems to meet the threat of determined violent assaults.

Because of the number of facilities, some uniform training program may be required.

Large differences may exist in the training program of local law enforcement agencies who provide response force capabilities to nuclear facilities. Inasmuch as the protection of nuclear materials involves considerations which are quite different from those encountered in routine police activity, specialized education and training would seem to be most helpful.

The breadth and detail of the policy issues enumerated above indicate the extent of staff work and coordination required to establish agency positions and complete supporting administrative and regulatory actions. The task force estimated that normal, routine activity could take up to two years to resolve these issues if the upgrading program were contested. The additional time required for the licensees to develop their detailed safeguards plans, for ERDA and NRC review, plus completing construction and plant modification is also estimated to be about two years. Thus, following normal, routine procedures, the total time for go ahead to completion would be about four years. This total time could be reduced to approximately two years by extraordinary effort that would enlist the full support of the licensees, compress the time to about six months for resolving only the most fundamental policy issues, allow the licensees about three months to complete their detailed planning, three months for ERDA and NRC to review and approve individual plans, and about twelve months for construction and facility modification.

Interim measures could be employed to provide some measurable improvement in safeguards capability during either the compressed two-year or routine four-year program. The question of interim measures is again a matter of judgment as to the urgency and scope of safeguards improvement that may be warranted before the upgrading program would be completed on either the two- or four-year schedule. Interim measures that would lead to improved guard capabilities include: use of commercially available semi-automatic weapons that could increase firepower without violating current legal constraints; improved or more extensive training that would encompass adversary and defensive tactics, communications, and defensive planning; and increased numbers of guards to increase surveillance and response capabilities. An interim measure to increase capabilities against internal conspiracies would be expediting a program of security clearances based on full-field background investigations for key personnel. These are measures that could be implemented in a short time, would result in immediate improvements in safeguards capabilities, and would not have counterproductive effects on meeting the overall upgrade.

Program Disclosure

When program decisions are reached on design threat levels, schedule, and the financial and regulatory approaches, a decision will have to be made whether or not to disclose the nature and extent of the program at the outset. The licensees have an early need for all information relevant to the design of cost-effective safeguards systems. If the licensees are given a series of

orders to improve safeguards without knowing the extent and end objective of the program, they are likely to resist what they view as an open-ended program of ratcheted safeguards requirements. Some licensees may need an early and full disclosure of the program to make judgments whether or not to remain in the business. That judgment is likely to be colored by their capital requirements and the prospects for financial assistance with the capital outlays required for safeguards upgrading.

Financing

The financing of additional safeguards measures is a major concern to participating licensees. Financial concerns are focused on both the initial capital outlays and the reimbursement of recurring costs (including operating costs and depreciation of initial investment). Cost reimbursement poses little problem for licensees heavily committed to ERDA contracts; financing initial outlays could pose a problem for all licensees. Some have said that they consider meeting high confidence protection against determined violent assaults to be a responsibility of the government. Without government assistance on financing the increased costs, they may request hearings or initiate court suits to resist the upgrading actions.

ERDA has an acknowledged obligation in assuring that its contractors achieve the required level of safeguards capability. For those facilities providing services to the government under cost-type contracts, or fixed-price contracts with provisions for equitable adjustments if safeguards requirements change, reimbursement of recurring safeguards costs would be available within

the framework of the existing contracts. For companies under new contracts negotiated during a period of substantial safeguards changes and the attendent requirements for new capital investments, financial assistance might be in the form of guaranteed loans, progress payments or advance payments.

The cost of compliance with regulatory requirements is a normal legal responsibility of the facility operator, including those licensees providing services under fixed-price contracts with no equitable adjustment provisions, as well as those licensees not providing contractual services to the government.

The task force assembled cost figures from the industry proposals into a rough estimate of total initial costs to facility operators of $20-25M, and $10-15M for annual operating costs. Costs to facilities which are largely devoted to ERDA contracts amount to roughly 60% of the above totals; almost all the rest of the costs are at facilities which have both ERDA and private contracts.

Affected ERDA programs would budget for cost increases in FY 1978 and thereafter. Prior to FY 1978, if the affected programs are unable to absorb the cost increases, the remaining means of relief would include reallocating or reprogramming funds, which is always difficult. Reprogramming approvals by ERDA, OMB, JCAE, and House and Senate Appropriations Committees normally take one to two months.

In summary, the financing of safeguards costs is an expressed concern of the licensees, some of whom may initiate litigation to resist additional

safeguards requirements if adequate financing arrangements are not made. For several current contractors, ERDA expects that existing authority will be adequate to handle both the initial financing and cost reimbursement of upgraded safeguards and litigation is not expected. Responsibilities for and means of financing safeguards costs for the licensees who do not currently have ERDA contracts are more difficult to determine. The task force believes that questions of responsibility and financing should not, in principle (but in fact), hinder a speedy program to improve safeguards. The specific methods and schedules of financing can be resolved only when detailed planning is available to provide adequate schedules, cost estimates, and definitions of responsibilities. But the general philosophy and approach to financing safeguards upgrading may require early resolution, before the licensees are required to prepare detailed plans. Otherwise, they may be provoked into legal resistance that will effectively impede a deliberate upgrading program.

Regulatory Issues

The site reviews indicated that the licensees were generally in compliance with NRC safeguards regulations, but the weaknesses found in overall performance (when evaluated against assumed threat levels) indicate that compliance with the present systems and procedural requirements does not necessarily equate to safeguards capabilities. Augmentation of the current regulations with general performance requirements may be desirable to assure a continuing obligation on the part of the licensees for maintaining the current improvements in safeguards capabilities.

If the desired level of upgrading represents a major departure from the industry's current capabilities, a number of issues must be addressed. Promulgating new safeguards requirements requires the preparation of an environmental impact assessment and possibly an environmental impact statement.

The approach chosen for imposing requirements for upgraded safeguards capabilities would partially depend upon the time required to attain those capabilities. Once a set of license conditions has been drafted, specific licenses can be modified immediately by issuance of amending orders. Alternately, the rulemaking procedures involving public comment and normal review is estimated to take from six months to two years. An immediately effective rule, with accelerated internal review, could probably be in place within six months.

Performance-oriented safeguards requirements may introduce problems related to both license review and approval and to legal enforcement. A phased review and approval process might be structured as follows:

1. NRC issues requirements expressing performance capabilities and the techniques that will be used to evaluate licensee response, e.g., onsite evaluations, blackhat analysis.
2. Licensees submit detailed plans and proposed procedures.
3. NRC reviews plans and procedures for adequacy of safeguards and issues conditional approval.
4. ERDA reviews plans and procedures for cost effectiveness and possible production impacts.

5. Site reviews, inspections, and other techniques, defined in the requirements, are used to change the conditional approval to full approval based on the assessed effectiveness of the implemented plan.

Continued and frequent inspection and testing for effectiveness would follow full approval. A mechanism to incorporate changes to the plans would also be needed.

VII. FINDINGS AND RECOMMENDATIONS

Findings - Current Safeguards

With some exceptions, the 13 NRC licensees who now possess SSNM are currently judged to have safeguards adequate against theft or diversion by an assumed internal threat of one employee occupying any position or an assumed external threat comprised of three well-armed (legally obtainable weapons), well-trained individuals, including the possibilities of inside knowledge or assistance of one insider. The exceptions are:

- Two facilities are vulnerable to both the external and internal threats postulated.
- Four facilities are vulnerable to the postulated external threat.
- One facility is vulnerable to material diversion by the internal threat of a single employee.

These exceptions are being resolved voluntarily by the licensees or by the imposition of additional or more specific license conditions on a case basis. Some of the corrections could be made more efficiently through longer term facility improvements, but adequate short term fixes are available. These corrections are planned for completion by August 1976, without a major impact upon the industry as a whole, although they may be viewed as significant to several of the licensees.

The above exceptions were discovered by means of performance assessments at each facility. In general, the licensees were found to be in compliance with current NRC regulations. In many cases it was apparent that the licensees

were complying with the technical requirements of NRC regulations rather than looking toward their actual safeguards capabilities. Thus, there is no assurance that the current safeguards posture will be maintained by the licensees in the absence of imposing performance requirements as an integral part of the licensees' obligations. Such additional performance requirements could be imposed by order, license conditions, or by regulations. They could supplement the current requirements for safeguards systems and procedures and could provide some basis for prompt action if licensees fail to maintain their current safeguards capabilities.

Conclusions from the comparative safeguards evaluations at three representative ERDA facilities were:

- Present capabilities are more than adequate against an unassisted external threat level assumed in this review.
- The facilities could not, with a high degree of assurance, protect against an external force in possession of inside knowledge or assistance and operating in a covert manner because of inadequate, marginally effective detection aids.
- One facility could not, with a high degree of assurance, prevent the diversion of significant quantities of SSNM by an insider. Improvements were needed at all three facilities in the techniques used to prevent the diversion of significant quantities of SSNM.

As an interim measure, the noted deficiencies were corrected by short-term actions. Each of the facilities is presently judged to have the capability to effectively counter the external or internal threat levels used as review criteria

Findings - Upgraded Safeguards

While the task force believes that the industry safeguards posture can be substantially upgraded, it is not clear that all of industry is prepared or willing to participate. Some members of industry assert that they do not have the technical backgrounds or disciplines necessary to design and operate safeguards systems against determined violent assaults, while others indicated a philosophical reluctance or unwillingness to maintain safeguards of this character. These reservations stem, in large part, from their perceptions of the relative roles of industry and government for the protection of nuclear materials against such threats. Such reservations were most noticeably held by the larger, more diversified companies. Financial and legal concerns are also evident. Less concern was expressed with regard to internal conspiracy threats.

It is technically feasible to upgrade industry safeguards to defend against internal conspiracies and determined violent assaults. Such an action, however, would be difficult and time consuming. The upgrading could require up to four years if accomplished through normal regulatory and financing procedures because of delays inherent in formal regulatory and budgetary processes as well as anticipated industry reluctance and difficulties in raising needed capital.

The minimum time required to put the upgraded safeguards into place without resorting to emergency (and possibly counterproductive) methods is about two years. This schedule would permit about six months for government

to prepare the regulatory, financial, and design bases for the upgrading; about three months for industry planning and design; about three months for NRC and ERDA to review and approve plans; and up to about twelve months to execute the needed actions. In order to achieve the desired level of safeguards within this two year period, the task force believes that it will be necessary to employ the most expedient regulatory means available and provide initial funding to the licensees to enable them to initiate the needed capital improvements. The regulatory requirements could be imposed either by immediately effective rule or by license conditions. The amount of financial assistance and the timing of its availability will affect the timing of implementation actions. Without initial financing, some licensees are almost certain to oppose the upgrading requirements and could contest their necessity or propriety in court or in hearings. Although there is some industry reluctance to assume responsibilities for protecting SSNM against larger threats, the task force believes that most licensees would voluntarily accept substantially increased levels of safeguards if initial financial assistance were made available. The task force considers this industry acceptance a fundamental determinant of the ultimate quality of the safeguards.

There are several immediate actions available which could be used to provide additional protection in the interim period prior to full implementation of an upgrading program. Guard performance could be improved by upgrading armament, training, and numbers. Equipping licensee guard forces with commercially available semi-automatic weapons would increase firepower without

violating current legal constraints. Safeguards effectiveness could also be enhanced by requiring all guards to be trained in accordance with an NRC syllabus of training, similar to that currently being provided guards and drivers for transporting SSNM. A third means of improving safeguards is by increasing guard numbers; however, an increase in numbers without also improving guard quality (armament and training) is not likely to add much capability against determined violent assaults. Furthermore, a brute force solution of forcing the licensees to increase guard levels beyond those required or appropriate for the final safeguards posture would likely meet considerable industry resistance and be counterproductive. A final interim measure would be to approve a program by which selected licensee employees would be granted clearances based on full-field background investigations. Such a program might be similar to that currently used for access to classified information and should provide substantial protection against internal conspiracies. The task force believes that any immediate, interim measures used to upgrade safeguards should be applied equally to all licensees and should not exceed the extent of improvements that a licensee would be required to make as an integral part of any final upgrading solution.

An early and full disclosure by the government of its intentions to upgrade safeguards may be an important step in avoiding delays or resistance in implementing any significant upgrading program. If the licensees are not made aware of the upgrading program objectives and schedule, they may view the entire program as open-ended "ratcheting" and they could impede the upgrading by initiating litigation.

Recommendation - Current Level of Safeguards

The task force recommends that both ERDA and NRC take the necessary near-term actions to establish and then consolidate a safeguards posture for licensed facilities that will afford high-confidence protection against theft of SSNM by a single insider acting alone or by a small, lightly armed group of outsiders. These actions should include:

- Completion of the ongoing specific improvements identified by the ERDA and NRC site reviews.
- Establishment of functional capabilities expected of safeguards systems and procedures for the protection of SSNM, including explicit descriptions of the threat levels and criteria to be used in evaluating their performance.
- Follow-up performance reviews to assure that the required improvements have been accomplished and that the desired levels of safeguards capabilities are being maintained.

These actions should be scheduled for completion before the end of summer. The task force recommends that follow-up reports on the state of the safeguards posture for the protection of SSNM at licensed fuel cycle facilities be submitted in the fall of this year.

Recommendations - Upgraded Safeguards

The task force recommends initiating actions to upgrade the safeguards posture to a level affording high-confidence protection against theft of SSNM by internal conspiracies or determined violent assaults. This recommendation

is not based upon a perception of any imminence of threat to the nuclear fuel industry; rather, it is based upon the judgment of the task force as to what constitutes a prudent level of protection. Some persons may feel that the current level of protection is adequate; others certainly would not be satisfied without levels of protection greater than those recommended. The task force believes that the upgrading of safeguards to these capabilities should be implemented as rapidly as possible, consistent with sound technical and policy decisionmaking. In the absence of evidence of serious threats to the industry, the task force does not believe that emergency measures, such as shutdown of the industry or the immediate use of federal forces, is warranted. On the other hand, the volatility of the threat situation with respect to the nuclear industry and society suggests that upgrading should be accomplished more quickly than by normal routine action.

The task force recommends that:

- NRC initiate within six months the following interim measures to upgrade safeguards:
  - Institute a program of clearances based upon full-field background investigations for selected licensee employees who might effectively conspire to steal or divert SSNM.
  - Require licensee guards to be armed with semi-automatic rifles.
  - Define and require a training program for licensee guards to insure an adequate knowledge of their duties and responsibilities.
  - Insure that all licensees have sufficient numbers of guards to defend against attempted armed robbery by small groups of persons.

- NRC complete the following actions within six months:
  - Resolve the need for employment constraints, if any, and establish requirements for the employment qualification of guards whose duties include defense against determined violent assaults.
  - Determine the utility of automatic weapons in the defense of nuclear facilities and, if judged necessary, initiate appropriate measures to permit their use by licensees.
  - Make an initial environmental impact assessment for the proposed upgrading program.
  - Establish, using the most expeditious regulatory means, the requirement to defend against internal conspiracies and against determined violent assaults.
  - Establish methodology and procedures for inspecting and enforcing the performance requirements.
  - Provide the means for each licensee to have access to classified information pertinent to the protection of their facilities.
- ERDA and NRC:
  - Disclose the intent to upgrade safeguards within two years to defend against both internal conspiracies and determined violent assaults.
  - Complete within 12 months the review and approval of all necessary facility modifications and security plans for upgraded safeguards, including cost estimates.
- The potential impacts of capital expenditures required to upgrade safeguards be carefully considered for all licensees, including those without ERDA contracts.