SECRET

This document consists of 81 pages
No. 10 of 15 Copies, Series C

NOV 11 1974

NOV 11 1974

Classified by:
Vance H. Hudgins
Assistant Director
for Politico-Military
Security Affairs

The President
The White House

Dear Mr. President:

In accordance with NSDM-255, an Ad Hoc Group, chaired by a representative of the Atomic Energy Commission and comprising representatives of the Department of Defense, the Department of State, the Central Intelligence Agency, and the Arms Control and Disarmament Agency, has prepared the enclosed study concerning possible provisions for an international convention concerned with physical security of nuclear weapons materials (plutonium and highly enriched uranium.) We focused on the importance of obtaining international consensus, on the need for physical security of nuclear weapons materials in situ and in transit, on the need to define certain elements of international cooperation relative to such security, and on various approaches to obtaining international adoption of such security measures as may be agreed.

It was realized that most countries may recognize the dangers but many may be reluctant to accept obligatory international inspections or enforcement of standards. Given that, we considered a spectrum of alternatives ranging from a convention with stringent, specific guidelines and mandatory international inspections to a convention with more general guidelines and essentially voluntary provisions. International acceptability is likely to increase as one moves away from the specific toward the more general convention, and concurrence is much more likely without a requirement for verification. The details of the approaches considered are set forth in the attached executive summary of the interagency report and in the report itself.

The study recommends that you approve the following approach:

1. Drafting by the IAEA and negotiation of an international convention by which a large number of countries would subscribe, at least in principle, to adequate and effective physical security standards which conform to the extent practicable with specific international guidelines.

2. U.S. initiatives for the adoption of common policies by the key suppliers to assure adherence to the convention through their bilateral assistance agreements with recipients.

SUBJECT TO GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652 AUTOMATICALLY DOWNGRADED AT TWO YEAR INTERVALS AND DECLASSIFIED ON DEC. 31 1982 (insert year)

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions.

SURNAME

DATE

SECRET

Form AEC-318 (Rev. 9-53) AECM 0240 GPO 920-284

We recognize that such an approach will require a flexible and carefully executed plan of action and that proper timing is critical to its successful execution.

It should be noted that there are a number of related activities currently under way that are directly supportive of or complementary to the above approach. Of primary importance, the NSSM-202 study of U.S. Nuclear Non-Proliferation Policy, which is nearing completion, will recommend an overall strategy which includes consultations with other nuclear suppliers to obtain concerted action in a number of critical non-proliferation areas, including physical security. In addition, the following specific actions related to physical security have been taken or are currently in progress:

-- The Secretary of State, the Director of ACDA and I, along with senior members of our staffs, have begun preliminary bilateral discussions with representatives of other key supplier countries on non-proliferation policy issues, including physical security.

-- Recent appeals for international action on physical security have been made by the Secretary of State at the UNGA, and by me before the IAEA General Conference in September.

-- The Atomic Energy Commission has published regulations and regulatory guides covering physical protection of nuclear plants and materials within the U.S. We also adopted the policy that no new commitments or contracts will be made to supply foreign countries significant amounts of nuclear weapons materials (plutonium or highly enriched uranium) unless adequate physical security arrangements are assured.

-- The Atomic Energy Commission is holding technical discussions with nuclear supplier and user countries on physical security measures, including current standards, R&D, and future plans. This will encourage maximum cooperation and exchange of information.

In line with the NSSM-202 study recommendations, NSDM-255 guidance, and other non-proliferation activities currently under way, we recommend the following additional actions for implementing the approach outlined above:

a. The AEC will continue detailed technical discussions on physical security questions with nuclear suppliers and users.

OFFICE ➤						
SURNAME ➤						
DATE ➤						

b. The Department of State, in coordination with the AEC and ACDA, will continue to hold discussions regarding concerted supplier actions with other supplier countries. In the course of these discussions, we will surface on a highly confidential basis with the UK, Canada, the FRG, the Soviet Union and France our approach to physical security as outlined above, and seek their support.

c. The U.S. will undertake initiatives to assist the IAEA to draft an international convention on physical security standards, and to promote widespread international adherence. The U.S. might also pursue an UNGA resolution agreeing, in principle, to the need for physical security measures and assigning follow-on action to the IAEA.

d. Once the above steps, including the negotiation of an international convention, are accomplished, we would urge the key suppliers to adopt a common policy regarding physical security and to develop the mechanics necessary for the imposition of adequate physical security measures by the suppliers on the recipient countries.

We will continue our related activities as discussed above pending your review and approval of the recommended course of action.

Respectfully yours,

Original signed by
Dixy Lee Ray

Chairman

SECRET

NSDM 255*

that part dealing with

STUDY OF PROVISIONS FOR AN INTERNATIONAL CONVENTION CONCERNED WITH PHYSICAL SECURITY GUIDELINES AND TRANSFER OF MATERIALS, EQUIPMENT AND TECHNOLOGY

Prepared by an Ad Hoc Group composed of representatives of the:

Atomic Energy Commission, Chairman
Department of State
Department of Defense
Arms Control and Disarmament Agency
Central Intelligence Agency

September 1974

*NSDM-255 "Security and Other Aspects of the Growth and Dissemination of Nuclear Power Industries," June 3, 1974

When separated from enclosures, handle this document as UNCLASSIFIED
(Insert proper classification)

Document Transmitted Herewith Contains NATIONAL SECURITY INFORMATION

SECRET

TABLE OF CONTENTS

A. EXECUTIVE SUMMARY

Purpose: This report is in response to NSDM 255,* dated June 3, 1974, which directed, in part, an Ad Hoc Group to study "possible provisions for an international convention concerned with physical security guidelines." The NSDM also directed that the Ad Hoc Group "explore the idea of establishing better information exchange internationally on transfers of materials, equipment or technology."

Background: In NSDM 255, the President approved the following actions which the Under Secretaries Committee (USC) had recommended in response to NSDM 235 concerning "steps the United States could take with other nations concerning the problems associated with the increased availability of weapons usable materials from the growth and dissemination of nuclear power industries":

1. That the U.S. initiate consultations with other countries--particularly present or potential suppliers of materials, technology, and equipment--with the objectives detailed in the USC report. The initial consultations should emphasize but not necessarily be limited to the need for: (a) establishing agreed international guidelines, preferably based on U.S. practice, to ensure the physical security of weapons usable and highly toxic materials whether internationally transferred or indigenously produced; (b) reaching some common principles regarding the supply of sensitive enrichment technology or equipment; (c) avoiding or applying stricter terms for supply in situations where special hazards could be present; and (d) encouraging, where appropriate, multinational enrichment, fuel fabrication and reprocessing facilities.

2. That a prompt study of possible provisions for an international convention with physical security guidelines be conducted by an Ad Hoc Group, chaired by a representative of the Atomic Energy Commission, and comprising representatives of the Departments of State and Defense, the Central Intelligence Agency, and the Arms Control and Disarmament Agency. In addition, the Ad Hoc Group should explore the idea of establishing better information exchange internationally on transfers of materials, equipment, or technology.

The studies directed in paragraph (2) are the subject of this report; however, it is recognized that the consultations directed in paragraph (1) are closely related and a necessary prerequisite to the establishment of an international convention.

---

*"Security and Other Aspects of the Growth and Dissemination of Nuclear Power Industries," June 3, 1974 (Appendix A)

A distinction must be drawn between international safeguards which are directed toward detection of and preventing diversion of materials at the national level on the one hand and physical security measures to protect against theft or sabotage by subnational groups on the other. The objective of IAEA safeguards is the timely detection of diversion of significant quantities of nuclear weapons material from peaceful purposes and the deterrence of such diversion by risk of early detection. A review of IAEA safeguards, their role, status, effectiveness, and relationship to the NPT is attached in Appendix E. The IAEA does not now have responsibility for physical security. Each member State is charged with maintaining a materials accountability and control system; however, physical security measures are left to their discretion. IAEA has published physical security guidelines for voluntary use by the member States (Appendix C).

<u>Discussion</u>: Physical security measures are considered necessary to prevent acts of theft or sabotage. The U.S. has already published physical security regulations (Appendix B) and is continually upgrading them with the changing threat. The Ad Hoc Group believes that standards for physical security measures should be adopted internationally and should, if possible, be as stringent as current U.S. standards. The establishment of adequate physical security measures on a global scale is extremely important as a supplement to IAEA safeguards. The Ad Hoc Group believes that an essential element in achieving this goal is common views as to desirable domestic systems in major nuclear industrial states and subsequently agreement among supplier countries to enforce stringent physical security measures through bilateral agreements with recipient countries, in the absence of international agreements.

In addition to national physical security measures, consideration must be given to necessary elements of international cooperation relevant to physical security. These include improving exchange of any relevant advanced warnings of theft, commitments to respond to requests for cooperation in the pursuit and recovery of stolen material, understandings as to responsibility for physical security during international shipment, and a commitment to share information on physical security systems. In this regard, we believe that international procedures should be established concerning detection and pursuit of offenders, recovery of stolen nuclear materials, and extradition and prosecution of persons accused of theft of materials or sabotage of civil nuclear facilities. The establishment of a mechanism or adoption of existing mechanisms for timely exchange of information within agencies of the U.S. and with other governments is also necessary to cope with the problems of theft. These channels could also prove useful in coordinating pursuit and recovery efforts in case of a successful theft of materials.

Three international approaches to the problem of physical secruity were considered:

1. <u>Bilateral</u> where the U.S. could make supply of materials conditional upon establishment of acceptable physical security measures. This would not afford protection of materials already possessed, material which may be acquired from non-U.S. sources, or material produced in a State. Therefore, a broader approach is required.

2. International Convention by which a large number of countries would subscribe, at least in principle, to the goal of adequate and effective physical security guidelines.

3. Multinational Suppliers Agreement to enforce physical security measures through bilateral arrangements with recipient countries. This would presuppose adequate application of physical security in the supplier States and a common view of the international problem.

All international organizations with a reasonable connection with this problem have been included in this study. Factors considered included the extent of global coverage, relevance to past and current involvement in related issues, effectiveness, ramifications, and whether or not such a forum could expedite agreement on a physical security convention.

A projection of the postulated attitudes of other nations on an international convention shows that:

1. There is recognition throughout the world of the dangers inherent in having nuclear weapons materials fall into the wrong hands.

2. Most countries will be willing to take appropriate physical security measures and will agree with recommendations for security standards.

3. Many countries may not agree to obligatory international inspections or enforcement of standards.

4. Most countries will be willing to reach agreement on appropriate cooperative international arrangements related to physical security.

5. The PRC will not participate.

6. France, India, and the Latin American countries may resist a convention which limits their freedom of action.

U.S. Options and Tactics in Orchestrating a Convention:

In an International Agreement on Physical Security there are trade-offs between negotiability and stringency in several key areas. These produce a spectrum of alternatives ranging from a "hard" convention with stringent and specific guidelines and mandatory international inspections to a "soft" convention with essentially voluntary provisions. International acceptability will increase in moving from "hard" to "soft" provisions.

The possibility of using a subsequent agreement among suppliers as a mechanism to (a) induce wider adherence to a "hard" convention, or (b) enforce impelmenting requirements on the parties to a "soft" convention, adds additional alternatives.

The following options were considered:

1. A "hard" convention containing precise and stringent provisions concerning physical security measures, international inspection, and cooperation in recovery and prosecution.

2. A "hard" convention as in option 1, and a subsequent suppliers agreement requiring adherence or substantial conformity with the convention as a condition for further bilateral assistance agreements.

3. A "soft" convention, containing voluntary commitments to institute physical security measures which conform to the extent practicable with specific international guidelines, without international inspection, or inspection on a voluntary basis.

4. A "soft" convention as in option 3, to be followed by an agreement among key suppliers that bilateral supply agreements will contain specific mandatory provisions implementing the general obligations of the convention.

Conclusions: There is a spectrum of forms which a convention might take and the options discussed illustrate a range of possibilities. Although a convention with enforcement provisions appears unlikely to be satisfactory to many of the most important countries, the acceptance of a common view of the problem and internal application of physical security measures in those countries is a prerequisite to any international progress. Subsequently, we believe that obtaining effective physical security measures could rest in part in the achievement of a supplier's understanding. It is realized that this understanding is not assured and will require cooperation of several countries, most notably France. Moreover, effective supplier action should be non-discriminatory and this implies a willingness by the supplier nations themselves to accept such international controls as they impose upon their customers. Since many of the current key suppliers are also major recipients, initial consultations may be complicated by the possibility that they will react primarily as consumers. The bilateral consultations approved in NSDM-255 and now under way may provide initial indications of attitudes. It is our judgment that:

--many nations would resist a convention with mandatory provisions but might be receptive to a convention that is commendatory in nature;

--wide and effective implementation of standards depends upon acceptance and enforcement by the major user/supplier nations;

--in the absence of such a convention, however, such a common policy among suppliers to impose a stringent, mandatory, and thorough set of standards is likely to be seen as highly coercive and therefore politically objectionable to both suppliers and recipients.

--for this reason, a common policy among key suppliers with comprehensive and stringent standards, in the absence of a broad international agreement, is highly unlikely in the near term, although some important progress can probably be made in this direction;

--a broad international consensus on the need for physical security standards would provide a legal and political base for the adoption by suppliers of a common policy or imposing mandatory requirements; a convention would provide such a base.

If these judgments are correct, they suggest that the most effective approach to the goal of effective international physical security standards would involve first reaching a common view among the major nuclear states, and then an international convention and the adoption of common implementing policies by the key suppliers. In negotiating a convention, a possible U.S. tactic would be to advocate a fairly "hard" convention initially but be prepared to move toward softer provisions as required. Since we believe that a suppliers' understanding is a more likely means of achieving rigorous enforcement than an international convention, our objective should be to achieve wide international acceptance of the convention, on the hardest terms which will permit that result.

In addition to physical security standards, the convention should also include provisions concerning pursuit, recovery and prosecution in the event of a theft of nuclear materials or sabotage to nuclear facilities. While provisions of this kind may be politically sensitive, we believe such procedures are highly desirable and may be more widely acceptable to most nations than obligations dealing with physical security standards.

We favor the UNGA as the appropriate forum for proposing a convention, although debate on this issue should be avoided. The IAEA is the appropriate forum for drafting and negotiating the convention. In addition to specific guidelines for physical security measures, the convention should also contain provisions on international procedures related to sabotage, theft, and recovery of nuclear materials.

The intelligence network and international bodies such as Interpol can possibly assist in the exchange of information related to theft and recovery of nuclear materials. Existing export control organizations such as the Zangger Committee already provide some information on transfers of materials and equipment and offer the opportunity of increased exchanges by expansion of membership and responsibilities.

Recommendations:

1. It is recommended that we adopt a two-step approach to deal with the physical security problem.

a. An international convention by which a large number of countries would subscribe, at least in principle, to adequate and effective physical security standards and procedures which conform to the extent practicable with specific international guidelines. This would include provisions for defining international procedures for pursuit, recovery, and extradition and prosecution in the event of nuclear theft or sabotage of nuclear facilities.

b. Adoption of common policies by the key suppliers to implement and enforce the convention through their bilateral assistance agreements with recipients.

It is also recommended that a detailed plan of action be undertaken which could include the following:

a. Preliminary discussions, as authorized by NSDM-255, with other major supplier countries on physical security, the supply of enrichment technology, multinational enrichment and reprocessing facilities. In the course of these discussions, we should surface on a highly confidential basis with the UK, Canada, the FRG, the Soviet Union, and France our two-step approach to physical security as outlined above. These discussions ultimately should be coordinated with extensive consultations on the technical aspects of the physical security problem and the methods which could be taken to strengthen procedures.

b. An appeal for international action on physical security in the UNGA, as was made by the Secretary of State on September 23, 1974, possibly including US support for the concept of an international convention. This might lead to a UNGA resolution agreeing, in principle, to the need for physical security measures and assigning follow-on action to the IAEA if it appears as a result of the above consultations that it would be useful to do so.

c. Multinational consultations with key suppliers to discuss common non-proliferation policies in such areas as technology transfer, additional special arrangements, etc., as proposed in NSSM-202. This could include discussion of common policies on physical security as a means of gaining high-level political support in this area. This might also provide an opportunity to discuss on a confidential basis with other key suppliers the two-step concept and the eventual imposition of specific physical security obligations by the suppliers.

d. Drafting of a convention within IAEA; initiative by the US and other suppliers to obtain widespread international adherence.

e. Agreement among the suppliers to assure adherence to the convention via bilateral supply contracts. The IAEA seems like the appropriate agency to conduct the enforcement provisions. We must await, though, the agreement with the suppliers before we make our final judgment regarding enforcement, since this matter is of prime importance;

f. Continuing US bilateral requirement for adequate physical security standards on recipient countries along the lines of the Israeli/Egyptian model whereby the Agreement for Cooperation in Civil Uses of Nuclear Energy called for agreed on measures for security of materials, equipment, and devices.

3. It is recommended that to ensure proper physical security measure are taken in the transfer of nuclear materials that diplomatic and commercial channels be used to exchange unclassified information relating to the transfer. In addition, intelligence liaison channels can be used where appropriate in exchanging unclassified information relating to thefts and the recovery of nuclear materials. A system of rewards may be adopted to assist in the pursuit and recovery of nuclear materials, both domestically and internationally.

4. U.S. strive for expansion of existing international agreements in control of nuclear exports, such as the Zangger Committee, to provide for better exchange of information on the transfer of nuclear materials and equipment.

5. Physical security standards comparable to those used in the U.S. should be the basis for acceptable measures adopted internationally and enforced in multilateral supplier arrangements, while taking into account published IAEA guidelines (Appendix C) and the special needs of other States as applicable.

B. STUDY OF POSSIBLE PROVISIONS FOR AN INTERNATIONAL CONVENTION CONCERNED WITH PHYSICAL SECURITY GUIDELINES

1. Review Of Related Material

The President, following his review of NSSM-150 (United States Policy on Transfer of Highly Enriched Uranium for Fueling Power Reactors), directed in NSDM-235 that an action program should be developed by the Under Secretaries Committee to consider the diplomatic and other steps the U.S. might consider taking with other nations, and in particular other supplier nations, "with regard to the security, non-proliferation, political and economic aspects associated with the increasing growth and dissemination of nuclear power industries, with particular focus on potential problems associated with highly enriched uranium."

This task was assigned to the NSC Under Secretaries Committee and the proposed action plan for implementing the program is reported in NSC U/DM-122. In considering the issues involved in NSDM-235, it became clear that plutonium, rather than highly enriched uranium, is the weapon material that will become available in the near term to many nations in sizeable quantities. However, in the future, widespread distribution of enrichment capability could make available supplies of highly enriched uranium from non-U.S. sources. Therefore, the Under Secretaries Committee expanded the scope of the study to include consideration of the establishment of agreed international guidelines, preferably based on U.S. practice, to ensure the physical security of all fissionable materials usable in nuclear weapons whether internationally transferred or indigenously produced, and on methods of encouraging all states to provide physical protective measures for nuclear related facilities.

The proposed action plan concluded that a U.S. effort to induce other nations to stiffen their standards of physical security might be greeted with reluctance and, in some cases, with open resistance, since many nations regard physical security measures for their own nuclear activities as essentially a national prerogative. Nevertheless, the need for creating adequate physical security measures to protect highly enriched uranium and plutonium and related facilities throughout the world from diversions, theft or sabotage is so pressing that the Under Secretaries Committee recommended, and the President in NSDM-235 has approved, the following actions:

a. That the U.S. initiate consultations with other countries -- particularly present or potential suppliers of materials, technology and equipment -- with the objectives detailed in the USC report. The initial consultations should emphasize but not necessarily be limited to the need for: (1) establishing agreed international guidelines, preferably based on U.S. practice, to ensure the physical security of weapons useable and highly toxic materials whether internationally transferred or indigenously produced; (2) reaching some common principles regarding the supply of sensitive enrichment technology or equipment; (3) avoiding, or apply stricter terms, for supply in situations where special hazards could be present; and (4) encouraging, where appropriate, multinational enrichment, fuel fabrication and reprocessing facilities.

b. That a prompt study of possible provisions for an international convention with physical security guidelines be conducted by an interagency Ad Hoc Group, chaired by a representative of the Atomic Energy Commission and comprising representatives of the Department of State, Central Intelligence Agency, Department of Defense, and Arms Control and Disarmament Agency. In addition, the Ad Hoc Group should explore the idea of establishing better information exchange internationally on transfers of materials, equipment, or technology.

The studies directed in paragraph (b.) are the subject of this report; however it is recognized that the consultations directed in paragraph (a.) are closely related and a necessary prerequisite to the establishment of an international convention.

In dealing with the question of physical security, a distinction is drawn between the physical security measures which might be required of a recipient country to protect against theft or sabotage by individuals or groups not associated with the government (subnational level diversion) on the one hand and those international safeguards measures directed against diversion by the government of the recipient country (national level diversion) on the other.

The detailed IAEA-NPT safeguards procedures are silent on matters of physical security other than to charge the state with the responsibility for establishing a materials accountability and control system; the IAEA does not now have the right to impose its physical security guidelines on member states or to verify compliance. Instead, the principal safeguards procedures developed to date for use by the IAEA have been designed to detect losses of material through inventory taking and checking of material balances.* These procedures are primarily aimed at deterring national level diversion through post facto detection of loss. Although safeguards and physical security are related and complement each other, this report concentrates on physical security aspects. Strong physical constraints are considered necessary in preventing overt acts of sabotage or theft at the sub-national level and in minimizing the threats of diversion that could occur while materials are in transit. The improvement and elaboration of adequate physical security measures on a global scale is extremely important as a supplement to the IAEA safeguards and control procedures.

However, physical security considerations alone may not be adequate protection against a determined, organized, domestic or international group which seeks to acquire highly enriched uranium or plutonium for criminal or political reasons. Therefore, further consideration must be given to ways of facilitating advanced warning of thefts being planned by such groups and the pursuit and

---

* See Appendix E for further discussion.

recovery of the fissionable material in the event of a theft. The establishment of a mechanism or the adaptation of existing mechanisms for the timely and orderly exchange of intelligence and counterintelligence information among the various departments and agencies of the U.S. Government as well as the utilization of the existing positive and counterintelligence liaison channels with foreign governments are deemed necessary to cope with this problem of theft. The same channels could prove useful in coordinating pursuit and recovery efforts in case of international movement of stolen material.

2. International Approaches to the Problem of Physical Security

There are a number of possible approaches to the goal of an international convention for physical security. This section considers these approaches and combinations thereof pointing out some of the advantages and also the difficulties to be expected in each case.

a. Bilateral Approach

The U.S., throught the extension of its bilateral agreements for cooperation in the civil uses of atomic energy, could make the continued supply of nuclear materials and technology contingent upon the establishment by the recipient nation of physical security measures acceptable to the U.S. Measures of this kind have been proposed by the United States in the current negotiations on the sale of power reactors to Egypt and Israel. While such measures would apply only to the protection of U.S.-supplied materials and nuclear materials produced in such facilities, this could result in overall increased security measures with added protection for all materials and facilities within the state. Nevertheless, there would be no positive assurance that material of other than U.S. origin or that facilities containing no U.S. material would receive adequate protection simply as a result of U.S. bilaterally-imposed measures. A number of problems are evident in a bilateral approach. For one, other nations likely will resent any attempts from the outside to impose standards in an area regarded as essentially one of national prerogative, especially if the standards are being imposed bilaterally, rather than by an international body such as the IAEA. And, since some provision will be necessary for supervising the security system to assure continuous compliance, the inspection program and any related sanctions will probably be quite onerous to most nations. Presumably, however, inspections required by bilateral agreements might be less objectionable if conducted by an international body (IAEA), under arrangements similar to those now in effect for trilateral safeguards under Agreements for Cooperation. In addition, negotiations on a bilateral basis would require flexibility in individual cases to accomodate differing economic, political and legal structures in the several states since no single set of standards would be applicable to all. The obvious complaint of less-favorable treatment is certain to arise under these circumstances unless individual understandings are of a classified nature.

Another question centers on the degree to which specific requirements would be spelled out in the agreements; the danger, of course, being that dissemination of complete security plans opens the way to the compromise of those plans. This would be another point for consideration in the protection of the confidentiality of physical security agreements.

The bilateral extension of our Agreements for Cooperation to provide physical protection for U.S.-supplied nuclear materials should receive our serious attention as an option immediately open to us. However, it must be recognized that, with the increasing worldwide availability of enrichment services, reprocessing, fuel fabrication and other nuclear facility capabilities, the position now occupied by the U.S. as the foremost supplier is being progressively diminished. Stringent, bilaterally-imposed protective conditions, in the absence of similar conditions by other suppliers, might result in some states turning from the U.S. to other suppliers for their materials, facilities and services, or toward the development of their own indigenous capabilities, the results of which would mean increased commercial competition as well as the erosion of our influence over the security standards which might be applied in other states.

It is obvious that the bilateral extension of our Agreements to provide physical protection for U.S.-supplied nuclear materials and facilities will not, of itself, afford the desired degree of protection to other nuclear materials and facilities already possessed or which in the future may be acquired from non-U.S. sources or indigenously produced. A broader approach to insuring an acceptable level of physical security over all weapons-usable material and nuclear facilities will be required.

b. <u>The International Convention Approach</u>

An international convention would, in principle, permit the negotiation and acceptance of a universal standard for physical security measures by all concerned nations. The convention might have some or all of the following objectives: (1) to make more officials in all countries aware that there is a need to take promptly adequate steps in the area of physical security; (2) to obtain legal commitments from supplier and recipient countries to comply with common international guidelines on physical security procedures to be followed; (3) to establish a mandatory mechanism for some form of international inspection and verification of compliance; (4) to obligate parties to prosecute or extradite persons attempting to steal nuclear materials or to sabotage protected facilities; and (5) cooperation in the recovery of special nuclear material. These objectives present different political and legal problems, and may require somewhat different approaches, and even different ones for different countries.

1) <u>International Security Guidelines</u>

It would be theoretically possible to negotiate a set of international physical security guidelines, and to persuade recipient and supplier countries to apply them without concluding a convention on the subject. However, there are several advantages for incorporating such guidelines into binding international agreements, 1) the parties will take them more seriously, 2) they will be more likely to make a genuine political and material commitment to enforcing them nationally, 3) they will be more diligent in preventing and correcting violations to avoid international criticism and 4) they will be less likely to withdraw from the arrangement without extremely compelling reasons. In addition, because the guidelines would be applied uniformly, they would not give rise to economic disadvantages to complying country.

For these same reasons, however, many recipient countries may be less willing to agree to relatively detailed, stringent guidelines if they were incorporated into binding international obligations than if they were commendatory. Many countries will view suspiciously any proposal to accept binding legal obligations to carry out international rules on such traditionally domestic problems as internal security and police functions. In this sense, there may be a trade-off between the stringency and specificity of the guidelines on the one hand, and the degree to which recipient countries would be willing to obligate themselves to carry them out on the other.

SECRET

However, there may be ways to reduce this dilemma. For example, one possible approach might be to obtain broad international agreement in an appropriate multilateral forum to a convention obligating all parties to take "appropriate" measures in specified areas against certain types of threats, taking into account and implementing to the extent practicable relatively specific and stringent international guidelines. Parties might also be obligated to report on the measures adopted by them and to consult with the IAEA on possible improvements in their procedures. It might then be possible to obtain a subsequent agreement among the major nuclear suppliers to require strict adherence to the guidelines by recipient countries as a precondition for further nuclear transfers. The United States would, of course, apply the same requirements in all future agreements for nuclear sales to other countries.

2) <u>International Inspection and Verification</u>

It would also be possible, in the absence of a convention, to put together an entirely voluntary mechanism for international inspection, under which, for example, IAEA personnel would be available on the request of any country to conduct an inspection of its physical security system and offer recommendations for its improvement. It is recognized that IAEA is not currently responsible for, or capable of, providing physical security inspections; however, with the backing of the member countries and the U.N., the IAEA could be given such a role.

The advantages of including a system of international inspection and verification in a convention would be to establish binding procedures and standards for inspection which countries could not circumvent or ignore, and to ensure regular and uniform inspection of all parties on an equal basis.

As in the case of physical security guidelines, there may be a trade-off between the stringency of inspection procedures and the degree to which many countries would be willing to accept binding obligations. Even if all military installations were completely exempt from inspection and verification, many countries would resist the entry of foreign personnel into sensitive nuclear facilities because proprietary information might be revealed.

Once again, it may be possible to achieve greater stringency in these procedures through an agreement among suppliers to require submission to bilateral or international inspection as a precondition for further sales or assistance. Effective international standards must be seen as basically non-discriminatory; this implies a willingness by the supplier nations to accept the same standards and international inspection arrangements that they jointly require of their customers. This problem is highlighted by the fact that most of the current and key potential suppliers are also major recipients. The degree to which the supplier nations are willing to accept international controls may in fact set the outside limits on the kind of international physical security regime that can be achieved.

3) Trial or Extradition of Persons Stealing Nuclear Material

The inclusion in an international convention of a requirement for the trial or extradition of persons stealing nuclear materials or sabotaging protected facilities would be designed to deter such acts by minimizing the possibility that terrorists could avoid prosecution by escaping to countries which would be politically reluctant to take action against them in the absence of a firm international legal obligation to do so.

In this respect, it would be similar to the anti-terrorism provisions in the Hague, Montreal and Protection of Diplomats Conventions. This requirement raises some of the same issues as those associated with hijacking and flow of drugs. Such a provision may generate intense political controversy, particularly if it is viewed as part of the general U.S. anti-terrorism campaign. It may, however, be more acceptable because nuclear theft or sabotage by terrorists has potentially far more disastrous and destabilizing consequences.

4) Cooperation in Recovery of Stolen Nuclear Materials

A convention might also obligate parties to cooperate in recovering stolen nuclear materials, and in informing one another promptly of any information on possible attempts at nuclear theft or sabotage involving other countries. Such obligations would be stated in a general manner in the convention, and thus implementation would depend essentially on the good faith and common interest of the parties. However, procedures and mechanisms could be instituted within existing international police organizations, such as Interpol, to allow for meaningful procedures for cooperation on recovery of stolen nuclear materials. A system of rewards may be adopted to assist in the pursuit and recovery operations, both domestically and internationally.

c. The Multinational Suppliers Agreement Approach

In addition to a purely bilateral approach by the U.S. or an international convention of supplier and recipient nations, another avenue for upgrading national physical security measures would be through joint agreement by key supplier countries to enforce stringent worldwide physical security measures through their bilateral arrangements with recipient countries. This would somewhat parallel the efforts of the Zangger Committee, a committee of supplier nations formed to determine export characteristics that would trigger IAEA safeguards.

An agreement on the imposition of physical security measures by supplier nations, however, has definite coercive aspects which make it rather different than the export controls under deliberation by the Zangger Committee. First, there is at present no supporting international organization charged with insuring compliance with physical security measures. (Although the IAEA is concerned with export of special nuclear materials as well as facility safeguards to detect national diversion, it has not officially recognized the Zangger Committee, although will probably acknowledge the export controls determined by the Committee.) Imposition of physical security safeguards is somewhat comparable to implementing constraints on export of technology, a concept which has been introduced into Zangger Committee deliberations but was rejected by some members as falling outside the purview of the NPT.

As a second point of difference, in the absence of any agreed international obligations in this area, the unilateral imposition of stringent physical security requirements by a consortium of supplier nations, as contrasted to export controls that would merely trigger safeguards, would probably result in open hostility of many recipient nations. This situation would, in turn, present a significant economic advantage to those supplier nations which chose not to be a party to such a suppliers agreement. For this reason, it would be essential that all key suppliers, especially France which currently is not a member of the Zangger Committee, be a party to such an agreement.

In lieu of universal acceptance of a convention specifying stringent and mandatory physical security standards and international inspection (a highly unlikely outcome), a joint supplier nations agreement to enforce such standards would probably be the only effective means of insuring compliance. Again, the major disadvantage of such an agreement is that its highly coercive character might make it objectionable to some supplier nations as well as recipient States. One possible solution to this problem, as indicated in the previous section, would be a two-step process:

a. an international convention that attempts to obtain agreement on a framework for universal application of physical security measures with as much specificity as practicable, but perhaps commendatory rather than <u>obligatory</u> in nature so as to induce most nations to sign and ratify the convention.

b. A subsequent suppliers agreement to insure that these standards are stringently enforced.

The value of this approach is that a commendatory convention would have a much greater chance of success than an obligatory convention; the convention would then serve as the legal-political basis for a subsequent suppliers agreement to enforce the convention.

A further problem concerns the difficulty of formulating uniform mandatory standards to apply universally without losing a great deal of their specificity, whether for use in an international convention or in a suppliers committee. Enforcement by the supplier through bilateral agreements could permit the physical security requirements to be tailored to the particular needs and capabilities of the recipient, but this appraoch might lead to recipient charges of discriminatory treatment by suppliers and in any event might erode the application of agreed and uniform standards.

An alternative might be to extend the mandate of the IAEA to encompass the negotiation of agreements with recipient nations containing explicit physical security standards and the supervision of their execution. The supplier nations would then impose a common requirement in bilateral agreements that recipient nations negotiate physical security agreements with the IAEA, similar to IAEA safeguards agreements. This approach would permit the IAEA to apply universal standards with some flexibility to meet varying national requirements, and might reduce the risks of erosion of the standards or discriminatory treatment. It is not without its own political problems however, as the experience of the IAEA in negotiating safeguards agreements attests.

3. <u>Postulated Positions of Other Nations on an International Convention</u>

Most countries of the world are expected to have no objection, in principle, to the draft standards on physical security provided they are commendatory in nature. There is recognition throughout the world of the dangers inherent in having fissionable material fall into the wrong hands, and most countries will be willing or have taken appropriate physical security measures to prevent such diversion. The PRC, however, will almost certainly not participate. There could also be problems with France and the Latin American countries. Although most countries would agree with recommendations for security standards, many would not agree to obligatory international inspections or enforcement of the standards.

<u>WESTERN EUROPE</u>. The energy crisis is leading to increased dependence on nuclear energy with attendant greater awareness of the possibilities of diversion, loss, or theft of nuclear materials. Many European countries are already sensitive to the problems of terrorism. Thus, it appears that most Western European nations would gladly accept some agreement on security measures. (France may be a problem and is addressed separately.)

<u>EURATOM</u>, as the nuclear supply agency of Western Europe, presents a special problem. There could be objections on any agreement which excluded or superseded EURATOM. Standards promulgated through EURATOM would probably be more acceptable to the Western European countries than bilateral agreements between the various countries and the U.S.

CONFIDENTIAL

Inspections or enforcement of security standards would probably be accepted, but grudgingly. The conduct of such inspections by an international organization such as IAEA would probably be more acceptable than U.S. inspections.

FRANCE. France will occupy a crucial position in any negotiations aimed at producing effective physical security standards. As a key supplier nation, her attitude may be the controlling factor in implementing such a convention. France is concerned about the vulnerability of her nuclear installations and is likely to support a fairly stringent convention, provided that it did not interfere significantly with normal operations, protected proprietary information, and was acceptable to most nations. However, any arrangement which threatens to weaken France's competitive position in the international market is likely to be strongly resisted. To gain the participation of France in any supplier's agreement enforcing the convention would probably be the most difficult and most important element in such an arrangement. EURATOM could play a role in gaining France's cooperation.

USSR AND EASTERN EUROPE. The Soviets are likely to be favorable to such an international convention. As long as the agreement is self-policing there will be no conflict with normal, very tight Soviet and Eastern European security. They would likely object to inspections. As a major economic power, the USSR recognizes its stake in world stability. Furthermore, the Soviets have a keen appreciation for the potential for abuse of nuclear technology, and take an active role in international efforts to limit opportunities for misuse of nuclear energy. The proposed convention would be consistent with such Soviet objectives.

CONFIDENTIAL

However, should Third World countries object strongly to the convention, Moscow might be reluctant to align itself for fear of being perceived as an overbearing superpower. On the other hand, should world reactions be favorable or neutral, and the PRC reaction adverse as expected, the USSR might support the convention even more enthusiastically in order to expose Chinese intransigency.

The Eastern European States will almost certainly follow the Soviet lead. They, like the USSR, are eager to reap the benefits of international nuclear cooperation.

ASIA

PEOPLE'S REPUBLIC OF CHINA. The Peoples Republic of China may very well oppose the proposed convention as another example of "superpower interference" in the internal affairs of others. There is virtually no chance that the PRC would participate in it. The PRC has not participated in previous nuclear conventions because she feels they are dominated by the two superpowers--the U.S. and the USSR--and might limit China's own nuclear program. Furthermore, Peking has made no public statement to indicate a concern in the area of physical security. Normal security in the PRC is probably much stronger than any which would be proposed internationally.

Republic of China. The ROC would probably readily accept the necessity for physical security standards. Due largely to the potential Peking threat, it maintains strict security standards now. The ROC might well, however, object to additional on-site inspections and consequent greater exposure of her nuclear facilities. Since the ROC is no longer an IAEA member, use of that forum to discuss and draft a convention could exclude her. But any attempt to include her could jeopardize the continuing--and extremely important--IAEA safeguards program on Taiwan which the PRC has already protested. For this reason, it would be best to handle the ROC aspect--if necessary--either through a bilateral program or a suppliers' agreement and avoid introducing the Chinese representation issue into efforts to conclude an international convention.

JAPAN. Japan also is expected to be in agreement with such an international convention, though they would not take the lead in its negotiation. Japan needs Western nuclear cooperation and could not afford to be cut off from such cooperation. Even though the Japanese nuclear program is growing rapidly, Tokyo has not shown as much concern about theft of fissionable material as might be expected. But Japan could resent the imposition of a highly detailed physical security program, preferring general guidelines with details worked out in Japan. She would also resent it if she were treated differently than Western Europe.

INDIAN SUBCONTINENT

INDIA. India maintains high standards of physical security in its large and growing nuclear program. She probably would have no objection to the proposed standards, as long as the policing is internal. But she would object strongly to anything which involved inspections, disclosures or other infringements of her sovereignty.

PAKISTAN. Pakistan would be expected to enthusiastically embrace the international convention. In the wake of India's recent nuclear test, Pakistan is strongly in favor of an international nuclear controls which would afford greater protection to non-weapon States. Furthermore, Pakistan's nuclear program is still strongly dependent on outside support, and she would probably go much further than India is allowing inspections in order not to alienate world opinion.

MIDDLE EAST

ISRAEL. Israel would probably agree to the world standards. Israel's bitter experience with terrorists has already forced her to very high standards of physical security. Such an agreement would have no real effect on Israel's normal practices in securing nuclear installations.

Israel almost certainly would object strongly to any inspection of her nuclear facilities. Nor would Israel be likely to provide access to information on Israeli security organizations or security plans for nuclear installations.

EGYPT. Egypt would probably accept the proposed standards. She might also allow inspection of the security arrangements on a periodic basis especially if the latter were tied to a similar agreement on the part of Israel.

IRAN. Iran can be expected to impose effective physical security standards to safeguard nuclear materials. Iran has had experience in the comparable areas of safeguarding both oil refineries and sophisticated weapons possessed by the armed forces. The Iranian National Intelligence and Security Organization (SAVAK) is a large, modern and reasonably efficient organization. The Shah is likely to associate nuclear programs with his own prestige and give top priority to safeguarding nuclear materials. As the Shah is keenly sensitive concerning national sovereignty, the Shah would probably not accept any form of inspection under a new convention.

SOUTH AFRICA. South Africa will probably support the convention on physical security. Although it has not signed the NPT, it politically supports the ideal of non-proliferation. South Africa has large uranium reserves and wants to enter the world market in enriched uranium. Furthermore, it needs international recognition to overcome an image as an international outcast. South Africa is likely to object to inspections of security arrangements at nuclear facilities.

WESTERN HEMISPHERE

CANADA. Canada is expected to support the international convention. Given Canada's strong position as an exporter of natural uranium and its current sensitivity to having been outmaneuvered in the nuclear arrangements with India, Ottawa might be particularly receptive to using the leverage to promote tougher physical security arrangements. This would be in keeping with its attitude on safeguards.

LATIN AMERICA. The Latin American countries--Argentina, Brazil, Chile, and Mexico--might be somewhat reticent about accepting such an international convention. Countries in which terrorism is a definite problem might welcome technical advice on security procedures and systems. But they would probably be suspicious of a convention which would involve outside scrutiny of their facilities or enforcement of standards, or which would limit their own initiatives in their nuclear programs. Their response would probably be predicated upon the responses of other nations with similar, fairly small nuclear programs.

4. Forums for a Convention

This section considers each of the international organizations that have some reasonable connections with nuclear materials, their physical protection, and/or recovery of any that are seized. As will be seen, other factors cause several of these organizations to be unlikely prospects for sponsoring a physical security convention.

Also included in this listing is the part each of these organizations has played in previous similar negotiations, as well as the relevance of the organization's membership to the problem of physical protection of nuclear materials.

a. United Nations-Authorized Ad Hoc Committee

The UN General Assembly can play a useful role in nuclear control, as it did in the case of the Non-Proliferation Treaty (NPT) by passing a resolution urging such an agreement and then endorsing the agreement. However, the General Assembly seems most unlikely to be able to provide a full working agreement itself, since the physical security problem is too detailed and scientific, as well as having controversial overtones of being an extension of the NPT.

The General Assembly could authorize an ad hoc committee for this purpose, but resort to such a committee would have many of the same technical and political problems ad direct action by the General Assembly itself.

Advantages of UN-Authorized Committee

1. Provides world wide attention to the problem being considered, both for public and for the governments.

2. Might involve France and the People's Republic of China (PRC), who have limited participation in most of the other suitable organizations.

Disadvantages of UN-Authorized Committee

1. The General Assembly might not authorize an ad hoc committee for the limited purpose of a convention on physical security.

2. Will provide opportunity for publicized attacks upon the associated NPT, particularly for any perceived imbalances between freedoms for nuclear weapon nations compared to restraints upon non-nuclear weapon nations.

3. The committee might become bogged down in such questions as national customs of policing or special status for para-military subnationals, e.g., Arab terrorists, or in criticisms of the arms control policies of the nuclear powers.

b. International Atomic Energy Agency (IAEA)

As the UN organization which is designated for atomic energy matters, the IAEA has specialized and knowledgeable staff and national representatives.

The IAEA is responsible for safeguards arrangements under Article III of the NPT, and physical protection can be viewed as a logical extension of this. Furthermore, the IAEA has already convened a panel of experts which produced "Recommendations for Physical Protection of Nuclear Materials."* This provides a precedent and a basis for further work by an IAEA convention (although nothing in the "Recommendations" by the panel of experts can be construed as requiring such a convention.)

To comply with usual protocol of the IAEA, approval for an IAEA physical security convention would first be obtained from the IAEA Board of Governors and would be followed by approval by the General Conference.

Advantages

1. Would include all IAEA members. However, the PRC has not yet accepted membership (although available) and the Republic of China (ROC) has been outed.
2. Effective people and a proper setting exist at the IAEA in Vienna.

---

*IAEA Vienna, June 1972. These new conditions are not binding upon the States. (Appendix C)

Disadvantages

1. As in the case of UN resolutions, anti-NPT spokesmen will have occasion to launch attacks upon the NPT, although not from so public a forum as the UN.

2. Also, as in the UN case, the IAEA could become bogged down in questions of national customs of policing or of paramilitary subnationals.

3. The ROC cannot participate, and the PRC is not now participating.

c. Consideration in the NPT Review Conference

The review conference specified in the NPT will be held in May 1975. In principle, physical security agreements could be considered at that time for inclusion along with the renewal of the NPT. Alternatively, it could be a separate agreement supplementary to the NPT.

For this May 1975 Review Conference, two preparatory meetings have already been held and a final one will probably be held in early 1975.

For physical security to be seriously considered in the May 1975 Review Conference, the U.S. position should be established by January 1975 so that preparatory discussions can be held with appropriate persons of other nations and with the IAEA.

Advantages

1. Nations already involved with the NPT are the most likely ones to cooperate in a physical security agreement.
2. Conceivably, although not likely, security requirements could generally be favorably received as an improvement of the NPT.

Disadvantages

1. The non-nuclear nations could make action on physical security a hostage for possible concessions they demand in the NPT renewal.
2. Many nations that are, or are likely to be, important producers of plutonium (Pu) or highly enriched uranium (HEU) are not participants in the NPT. These include France, the PRC, India, South Africa and Spain.
3. The time available for preparations might be too short.
4. The four weeks or less of this conference would likely be too short to negotiate a physical security convention.

d. Consideration in an Ad Hoc Group Commissioned by the NPT Review Conference

Rather than consider full aspects of a physical security agreement in the NPT Review Conference itself, an alternative would be for this conference to commission an Ad Hoc Group for this purpose. This would also need to be on the agenda for the May 1975 meeting, but the preparations would presumably not be so time-consuming.

Advantages

1. Same advantages as the 1. and 2. advantages in possibility (c.) for NPT review.
2. Adequate preparatory time is probably available.
3. The Ad Hoc Group could use whatever time is needed without prolonging the NPT Review Conference.
4. Conceivably, non-NPT nations could also be induced to join the Ad Hoc Group, although this seems somewhat inconsistent and therefore unlikely.

Disadvantages

1. Same disadvantages as the 1. and 2. disadvantages in possibility (c.) for NPT review.
2. Even some of the NPT participating nations might be disinclined to participate in such an Ad Hoc Group.

e. Conference of the Committee on Disarmament (CCD)

Following President Johnson's 1964 message on non-proliferation to the Eighteen Nation Disarmament Committee (ENDC), which was the precursor to the CCD, non-proliferation was the principal item on the ENDC agenda for the next three years. Thus, the NPT resulted largely from the ENDC.

The same forum could conceivably be used to achieve an agreement on physical security. However, physical security of nuclear materials is not clearly a disarmament subject, in contrast to the NPT. Thus, it is questionable whether physical security is a proper subject for the CCD.

Advantages

1. Being specialists in disarmament, the participants should easily be able to adapt to the issues involved in any compact on physical security of nuclear materials.

Disadvantages

1. The PRC is not a member and France is regularly absent, although a member.
2. A physical security compact has questionable appropriateness for the CCD.
3. The membership includes opponents of the NPT, who could use this opportunity to harm the NPT.

f. A Special Conference Convened by the UN

This would presumably be similar to the recent Law of the Sea Conference, the World Food Conference, or the environmental conference which treated problems of world-wide concern that require great attention. Both advocates and opponents actively participate.

Advantages

The problem would receive great and widespread attention. This might facilitate agreements, even if they follow after such a UN conference. All nations would be represented.

Disadvantages

1. The problem might not be sufficiently apparent to warrant the UN convening such a conference.
2. Such a conference, if it preceded or were held concurrently with the IAEA and the NPT Review Conference, could possibly harm both of these groups as well as harm the prospects of an agreement on physical security.
3. In such a conference, not only would representatives of any nation have the opportunity to attack the NPT through its association with the physical security problem, but the press and other groups would also have occasion to attack.

NOTE: The following fora are involved with nuclear materials and/or physical security, but do not appear to be suited for this physical security convention.

g. The Zangger Committee

The membership of this committee consists of the principal nuclear-supplying nations. This has been an ad hoc committee of some IAEA representatives, but meeting outside the auspices of the IAEA. The IAEA currently takes no position on the Zangger Committee decisions, but conceivably in the future the Director General of the IAEA might acknowledge the existence of the supply controls decided by the Zangger Committee, possibly without specifying this Committee.

h. IAEA Panel of Experts

The IAEA uses panels of experts for studies, one of them recently producing a report, "Recommendations for the Physical Protection of Nuclear Material." However, IAEA regulations restrict such panels to a small number of participants. Furthermore, the recommendations are not binding upon the member States.

i. International Criminal Policy Organization (Interpol)

In effect, this is a clearinghouse for information and for requests for assistance. Almost all nations are members. Headquarters are in Paris, and France supplies the local costs. The principal crimes with which it is concerned are narcotics traffic, counterfeiting, and smuggling, although Interpol is now branching to terrorism. Interpol does not deal with political crimes or espionage. Furthermore, the Interpol charter allows consideration only of individuals. Terrorist groups cannot be identified.

Being principally a clearinghouse for information and for requests for assistance, Interpol has no international agents.

Interpol might be useful in providing expertise for use in negotiating the provisions of a convention dealing with cooperation in the recovery of stolen nuclear materials, and the prosecution of offenders.

j. Other Regional Affiliations, Particularly EURATOM

As the nuclear energy organization of the European Economic Community, EURATOM includes some major nuclear States. Other regional organizations exist, although any nuclear subgroups they might have are not nearly as well established. These include the Organization of African Unity, Organization of American States, CENTO (Iran, Pakistan, Turkey, UK, and the US), Arab League, Warsaw Pact, NATO, and the Southeast Asia Treaty Organization. Any effort for a physical security agreement by combined effort with the necessary number of these groups would be very fractured.

5. POSSIBLE PROVISIONS FOR INTERNATIONAL PHYSICAL SECURITY GUIDELINES

Scope of Coverage

The primary purpose for pursuing an international convention on physical security in relation to the nuclear power industries is to ensure the physical security of weapons usable and highly toxic materials whether internationally transferred or indigenously produced. In order to achieve this broad objective, it is necessary to consider the question of the different ways that such materials could be illicitly used in the international environment.

For highly enriched uranium and for plutonium an immediate international threat is the theft of such materials by terrorists for their ultimate use in the fabrication of a nuclear explosive device. Another illicit use for plutonium and other radioactive fission products is to disperse them in specific geographic areas to create hazardous conditions for extended periods of time. A third category of illicit acts which involves sabotage to facilities in which radioactive materials are present and which could consequently result in the dispersal of such materials to the surrounding countryside. An act of sabotage to facilities handling materials for nuclear power industries, particularly such an act which results in significant casualties, would have political and public repercussions on an international scale in many parts of the world. As a consequence, it is assumed in this paper that such acts of sabotage are a part of the threat to be countered by physical security systems in international convention.

Basis for Using U.S. Standards as a Starting Point for an International Convention

The U.S., U.K., USSR, France, and the Peoples Republic of China are states with some longstanding experience in the area of physical protection related to their atomic weapons programs. Although all of these states would have considerable background in a physical protection system, it became clear during the development of the recommendations for the physical protection of nuclear material by the IAEA in early 1972 that only the U.S. was actively pursuing the establishment of rigid physical protection standards for its own nuclear power industry independent of any international encouragement.

The U.S. has published in the Code of Federal Regulations an initial set of physical protection requirements applicable to the private sector of the nuclear power industry. These requirements were supplemented by several guides describing in detail specific physical protection systems and procedures that could be used to satisfy the requirements established by the Regulations. None of the other states discussed above has published publicly such requirements. As a consequence, it is believed that these published requirements (together with certain upgradings under development and others now imminent) should be the preferred starting point for an international convention along with the recommendations for the physical protection of nuclear materials published by the IAEA in Vienna in June of 1972. The current published AEC requirements and associated guides are attached as Appendix B and the published IAEA recommendations are attached as Appendix C. The upgradings under development and those now implemented are discussed in subsequent paragraphs headed "Projected Improvements in Current U.S. Standards."

Objectives for Physical Security Systems

The objectives for a physical security system applicable to nuclear power industry on a worldwide basis can be summarized in the following ways:

- Protect facilities containing radioactive materials against industrial sabotage.
- Protect, against theft, types and quantities of nuclear materials usable as nuclear explosives.
- Protect radiological hazard materials in quantities and types usable as weapons against theft.
- Provide for the immediate detection of an act leading to the theft of materials discussed above.
- Provide for reaction mechanisms to neutralize an attempt to sabotage a facility containing such nuclear materials or to steal these materials.

- Provide to management the mechanisms to deal with a sub-national nuclear threat.
- Provide the capability to recover rapidly such materials which may have been successfully stolen.
- And finally, provide the necessary legal structure to bring sanctions to bear against any person or group attempting to commit an act of sabotage or theft against the nuclear industry.

A statement of the objectives in the above terms must precede any attempt to develop a set of agreed standards since specific measures to be included in a set of standards would be designed to deal with one or more of the above stated objectives.

Based on experience to date in the development of domestic standards in the U.S., there can be no compromising the above stated general objectives. Accordingly, it is considered essential that the first step for an international convention should be to arrive at an agreement on objectives which must as a minimum include those described above.

Current U.S. Standards

Following is a narrative discussion of the current U.S. standards applicable to the private sector (material attached as Appendix B). These in general focus on three of the four basic elements to a physical security system. The three that are dealt with are:

1. Access control mechanisms which are designed to provide assurance that only persons requiring legitimate access to facilities or to the materials within facilities will be permitted such access.
2. Removal controls which are measures designed to provide assurance that persons having legitimate access to facilities and materials therein do not surreptitiously remove such materials.
3. Response and recovery mechanisms which are measures provided to assure that efforts to breach either the access control or removal control measures will result in rapid reaction.

Such reaction would be designed to provide assurance that (1) the diverted materials cannot be used in a hostile way, or (2) if so used, the consequences in terms of public damage are kept to the lowest possible level.

The one additional factor which has not been incorporated in current U.S. standards because of a need for statutory authority (enacted August 1974) is that related to a prior determination by government authority to the trustworthiness of individuals who will be entrusted with the custody, control or protection of nuclear power industry facilities or radioactive materials involved therein. This prior determination by appropriate government authority as to the trustworthiness of individuals having such control is considered essential to any physical protection system. It is the only mechanism available to provide some assurance that individuals who might carry out an act of industrial sabotage or theft would have to breach an access control mechanism, which is also part of the facility protection system. They could not, for example, achieve their need for access to vital portions of facilities or the radioactive materials by easily obtaining employment especially if they have a history and record of illicit acts or are associated with groups with such a history or record.

Projected Improvements in Current U.S. Standards

The current U.S. standards are the product of an evolutionary system, and they are not considered to be the most effective standards. Nor are they considered to be completely adequate for the current or future industry. A number of improvements in these standards are currently under consideration by the AEC, the salient aspects of which are discussed in Appendix D.

Discussion of Provisions for an International Convention

Because of the evolutionary nature of the U.S. standards applicable to the private sector, it is believed that any international convention should adopt language which will permit flexibility. At the same time, if the convention is to result in a definitive set of physical security measures, the language should include specific, rather than general, guidelines. For this reason, the broad general language incorporated in the IAEA recommendations for physical protection (Attachment C) is not considered to be a completely adequate approach. However, this document may serve as a reasonable basis for the framework of an international convention.

The most essential features that must be included in a meaningful international convention are as follows:

1. The designation of an inter-governmental body to develop standards, approve their application and conduct periodic professional inspections (at least annually).
2. A system for prior determination of trustworthiness by professional government employees before individuals may have custody of or access to nuclear materials of concern.
3. A system of physical barriers (at least double sets of barriers for nuclear materials and for vital parts of nuclear facilities).
4. Firm access control procedures including positive identification systems.
5. Use of highly reliable alarm systems to detect unauthorized entry to protected areas.

6. Capability for dual communication from armed guard positions to backup forces.

7. Adequately planned backup forces capable of dealing effectively with an armed attack by small terrorist groups.

8. Dual armed guard protection for all transport of materials of concern.

9. Constant communication capability with highly reliable features for all transportation.

10. Preplanned recovery procedures, including international cooperation aspects, for diverted materials (should facilitate hot pursuit as well as more laborious search).

11. Establishment of a security organization at each site, including the use of armed guards and a program for thoroughly training the security force used in the system.

12. Procedures requiring observation of individuals who have access to materials of concern, e.g., buddy system or remote surveillance.

The goal of the international convention should be to describe detailed requirements and procedures to meet the above features at the strongest level possible, using the current U.S. private sector standards and the planned improvements thereto as a starting point. However, it must be recognized that circumstances in different states may be such that their ability to comply with an international convention would be determined by the flexibility of the requirements. For example, some governments may not be able to apply the trustworthiness determination procedures in the same degree of rigid detail as the U.S. may find appropriate. Accordingly, although the basic features enumerated above must be maintained, those responsible for negotiating the detailed language of the international convention should be prepared to accommodate such problems by including some flexibility in the language.

6. U.S. Options and Tactics in Orchestrating a Convention

As indicated in previous sections, there are possible trade-offs between negotiability and stringency in several key areas. These trade-offs produce a spectrum of alternatives ranging from a "hard" convention with stringent and specific guidelines and mandatory international inspection to a "soft" convention with essentially voluntary provisions for adopting physical security guidelines and for accepting international inspection and verification. In general, international acceptability is likely to increase in moving from "hard" to "soft" provisions. The possibility of using a subsequent agreement among suppliers as a mechanism to (a) induce wider adherence to a "hard" convention, and (b) enforce "hard" implementing requirements on the parties to a "soft" convention, adds an additional dimension to the alternatives.

The following options are illustrative of the extremes of this spectrum, with and without the second step of a suppliers agreement.

The Options:

1. A hard convention containing precise and stringent provisions concerning physical security measures, international inspection, and cooperation in recovery and prosecution.

Pros:

-- If it achieved wide acceptance, would produce maximum effective results in controlling physical security problem.

-- Would provide greatest opportunity to air the problems of physical security in all of its aspects, and in educating public and government officials.

Cons:

-- Prospects for wide adoption, or adoption by the most important countries, are extremely doubtful.

-- It could undercut U.S. leverage on non-proliferation matters by investing U.S. prestige in pursuit of unlikely objective.

2. A "hard" convention as in Option 1, with a subsequent suppliers agreement making adherence or substantial conformity with the convention a condition of further bilateral assistance agreements.

Pros:

-- If suppliers agreement achieved, would provide effective controls.

-- Same educative effect as in Option 1.

-- Avoids need for obtaining wide initial adherence to convention, and provides strong leverage for later adherence.

Cons:

-- Assumes agreement among suppliers which may be extremely difficult to obtain, particularly in case of France.

-- Coercive aspect may be highly objectionable to many nations, both suppliers and recipients.

-- Probably involves coercion of greater number of non-signatories to the NPT than in Option 4.

3. A "soft" convention, containing essentially voluntary commitments to institute "adequate" physical security measures which conform to the extent practicable with specific international guidelines, no international inspection, or inspection only on voluntary basis.

Pros:

-- Would stand chance of wide adherence, including ratification by key countries of present concern, committing most of the international community to the principle of providing adequate physical security protection to their nuclear facilities.

-- Might induce some countries to take effective measures.

-- Would have some educative and propaganda value in bringing issues to attention of governments and general public.

-- Might provide a basis on which to seek stronger measures at some later time.

-- Would be non-coercive.

-- Avoids practical problems of mandatory international verification machinery.

Cons:

-- Lacks specific commitments and means of verification, hence is less likely to produce much practical improvement in physical security beyond what countries willing to do anyway.

-- Might in practice merely provide veneer of respectability which allows some countries to do less than they might feel obliged to do in absence of a convention.

-- Could be used by supplier nations as an excuse for not imposing bilateral physical security requirements.

4. A "soft" convention as in Option 3, to be followed by an agreement among key suppliers that bilateral supply agreements will contain specific mandatory provisions implementing the general obligations of the convention.

Pros:

-- With respect to the convention itself, the first four pros of Option 3 above.

-- Would produce effective physical security measures in countries where suppliers agreement applied.

-- As compared to Option 2, reduces coercive implications of suppliers agreement, assuming much wider international acceptance of a "soft" compared to a "hard" convention, by permitting suppliers to claim that restrictions are in implementation of obligations undertaken in the convention and widely accepted by international community.

-- Coercive of fewer nations than Option 2.

-- If successful, might permit gradual introduction of international verification, reducing practical problems involved.

Cons:

-- Assumes suppliers agreement which may be extremely difficult to obtain, particularly in case of France.

-- Applies effective controls only to nations accepting new supply agreements. Discriminates in favor of nations with well-established nuclear programs.

C. ESTABLISHMENT OF INFORMATION EXCHANGE INTERNATIONALLY ON TRANSFERS OF MATERIAL, EQUIPMENT AND TECHNOLOGY

I. Introduction

In the Action Program, the Under Secretaries Committee concluded that controls confined to international transfers of plutonium or highly enriched uranium will be only marginally useful in helping abate the material aspects of the proliferation problem since the bulk of the world's plutonium will be produced by nations indigenously; and therefore international supply policies on the transfer of nuclear technology and equipment may be equally or more meaningful than restrictions placed on international transfers of plutonium or highly enriched uranium. It was recommended that consultations be held with other countries, particularly present and prospective suppliers, aimed at achieving agreement or understandings in the establishment of common principles and precautions concerning international transfers of nuclear equipment and technology.

NSDM-255 directed that we explore the idea of establishing better information exchange internationally on transfers of materials, equipment and technology. This section examines existing international controls on exports and liaison channels that might be used for this exchange of information, evaluates their potential effectiveness and prospects for successful implementation and identified expected problem areas.

The objective of establishing common principles and restrictions on international transfers of equipment, materials and technology is addressed in three areas:

1. establishment of better information exchange internationally
2. coordination of and cooperation in intelligence activities, and
3. establishment of agreements among supplier countries in controlling exports of certain technology, materials and equipment.

II. Better Information Exchange

With the rapid growth of nuclear power programs and the attendant increase in the amounts of fissionable materials throughout the world, it is becoming increasingly important for the United States as well as the rest of the international community to maintain a close surveillance of the actual transfers and location of critical equipment, materials and technology. Real time information exchanges among supplier countries could provide valuable assistance in promoting the objective of non-proliferation and in insuring adequate safeguards and physical security of special nuclear materials worldwide. The threat of theft or sabotage is probably most serious while materials are in transit. Information on the nature, quantity, route and destination of SNM would be a valuable aid to all countries affected. By alerting third countries over whose territory SNM is being shipped, such information exchanges could help in the protection and or the recovery of these materials. Such an inventory movement control might also assist in assessing claims of threat perpetrators regarding their acquisition of SNM.

Several problems arise in reaching agreements of this nature. Many nations may be reluctant to enter such understandings for fear that they may hurt their competitive position in the world market. Our approach to other suppliers on this question would have to clearly spell out that such exchanges would not include information of a commercial nature. We would have to stress the point that our exclusive interest in such a proposal would be to discourage proliferation of nuclear weapons and to increase the physical security of SNM while in transit internationally. Information exchange on the nuclear material transfer should be carried out by overt organizations, for example, the IAEA or by organizations involved in export control. Having IAEA play the critical role in this arrangement could help to reduce the commercial concerns of some countries.

The existing agreements on controls of exports as described later in this section provide some information exchange, and some, such as the Zangger Committee, might be expanded to include all major suppliers.

III. Possible Use of the Foreign Liaison Channels of the Intelligence Community

There are essentially two types of information exchange that could be conducted in the present foreign liaison channels of the intelligence community: One involves the exchange of counterintelligence information on potential threats of theft or diversion of nuclear materials; and the other is an exchange of information which might be necessary between governments to coordinate or assist in the pursuit and recovery of stolen nuclear material.

A similar extensive exchange of counterintelligence information on general international terrorist activities does now occur with many foreign intelligence and security services in support of the programs coordinated by the Cabinet Committee to Combat Terrorism (CCCT). Adding a "nuclear dimension" to such an exchange--assuming that governments controlling such services recognize the grave international ramifications of the nuclear physical security problem--would not appear to pose any great problem. We would, of course, expect differences in response from the various services, depending on their general cooperativeness, professional effectiveness, and alertness to the problem.

Whether or not the intelligence community should become involved in the pursuit and recovery effort is highly dependent upon the given situation. We do not believe any single information exchange mechanism now exists or is likely to be designed that can cope with the wide range of "theft scenerios" that have been discussed in the community. We can conceive of situations, particularly when great discretion is required, where our liaison with foreign intelligence and security services might be a very important or even the principal channel for cooperation. But, given other situations, particularly those in which the potential danger was great and appeared imminent, exchange might well be initiated at the highest government levels and could exceed the capabilities of any existing liaison with a local intelligence or security service. Use of diplomatic channels, country team participation, and even direct contacts among military services might be required. The foreign country or countries involved would also be an important factor, since liaison relationships differ in nature and degree of cooperation from service to service. In sum, intelligence liaison channels would certainly be a possibility in such a crisis situation. However, the nature and location of the crisis, the kind of information exchange required, and the extent of action to be taken based on that information would determine whether intelligence liaison channels should be employed or other routes followed.

IV. Establishment of Agreements to Control Exports

In its Action Program, the Under Secretaries Committee recommended that attempts be made to reach agreement or understandings with other potential suppliers on limiting transfers of sensitive enrichment technology to other countries. These understandings should indicate that such technology

a. preferably would not be internationally transferred to states not now possessing such technology except for use in multinational plants.

b. preferably would only be transferred to states that have signed the NPT (stipulating NPT signature as an absolute precondition in consultations with France or South Africa may be impractical since neither has signed the NPT), and

c. would be transferred only under specific agreements (1) to prohibit technology retransfer except as authorized by party supplying the technology, (2) to provide that the materials involved would be subject to IAEA safeguards, (3) to call for maintenance of secrecy on sensitive details of the technology, and where feasible, to prohibit or limit the production of highly enriched uranium.

Further, the Under Secretaries Committee concluded that the export of enrichment equipment should be subject to the same general restraints proposed for enrichment technology since a substantial degree of reverse engineering could serve to disclose technology. For this reason the inclusion of enrichment equipment on the Zangger Committee list should not be viewed as agreement that sale of such equipment is automatically acceptable when covered by IAEA safeguards.

Other countries should be encouraged to adopt suitable controls over the export of nuclear technology, including cooperation in the field of chemical processing where much of the information is unclassified and largely transferred to the private sector. The U.S. regulatory framework which is stated in the NSDM-235 Action Plan was recommended as a desirable point of departure.

Current International Agreements on the Control of Exports

The history of international agreements on controlling the export of technology, equipment and materials reveals many problems in negotiating and implementing understandings of this type. Several understandings or agreements exist among potential suppliers, and each has important limitations.

COCOM

Since essentially all potential proliferation problems are likely to occur outside of communist countries, there is little reason to attempt to pursue restrictions on nuclear technology, equipment and materials through the COCOM mechanism. However, an examination of COCOM can provide some insights into the potential and the problems of a similar arrangement among nuclear supplier countries.

Japan, as well as all of the NATO countries with the exception of Iceland, exercises embargo controls over an agreed list of commodities to communist countries. Most other COCOM members do not have strict systems of controls as does the United States; particularly in the area of reexports. For example, most appear to make little or no use of prelicensing or post shipment checks and indicate that they have no way to assure that their finished goods, parts or technology, after receipt by consignees in other non-communist countries, will not be reexported or utilized for other than the intended purpose. COCOM-established obligations for all member countries provide that their agreed commodity controls are not frustrated by exports of parts and technology to make COCOM products. These obligations are, however, of only a "so far as practicable," and "such action as it can" nature.

Many COCOM countries reportedly can only deal with violations committed within their borders, i.e., in connection with exports, not reexports, of their goods. All depend on criminal prosecutions or customs seizures. None has an administrative export denial procedure as in the U.S. And, as stated, only a few say they maintain black or grey lists.

Zangger Committee

The Zangger Committee is an informal, ad hoc group of delegates of fifteen states which are present or potential exporters of nuclear equipment and material. The principal objective of the Zangger Committee has been to establish guidelines on the export of materials and equipment to non-nuclear weapon states which are not party to the NPT in support of Article III.2. of the Non-Proliferation Treaty.

After some years of deliberations, the Committee was able to agree on only a limited list of items whose export would trigger the application of safeguards. Although the Committee has been useful in achieving agreement on this trigger list, it has been estremely difficult to put additional items on the list. Moreover, since Article III.2. of the NPT does not call for safeguards on technology trnasfers, the Zangger Committee's list does not include technology. Finally the membership of the Committee does not include several important suppliers of nuclear materials, equipment and technology. France is not a member and has not indicated whether it will abide by its list. Several members of the Zangger Committee have said that their final acceptance of the list will be dependent on French acceptance of the list.

Agreement with the Tripartite Countries

The Tripartite group (The Netherlands, FRG and UK) has made an agreement with the U.S. that they will classify and protect centriguge

CONFIDENTIAL

information similar to that protected by the U.S. Although we have no recent discussions with the group about the conditions under which they would export either enrichment equipment or technology, the international organization, Association for Centrifuge Enrichment (ACE) was established by the Tripartite to permit the export of both material and enrichment equipment or technology on a government-to-government basis to members of the association.

Ad Hoc Agreements

In a few instances, the U.S. Government has been successful in obtaining agreements from potential foreign suppliers to deny the export of technology and equipment to countries which would not accept international safeguards. For example, the U.S. succeeded in soliciting the cooperation of other supplier nations in denying exports of chemical reprocessing equipment to Taiwan because there was no assurance that international safeguards could be maintained in the Republic of China since it is no longer a member of the IAEA.

Energy Coordinating Group

The Washington Energy Conference (WEC) of February 1974 agreed on the need for a comprehensive action program to deal with all facets of the world energy situation by cooperative ventures. In establishin an Energy Coordinating Group (ECG) and an ad hoc group on international cooperation on uranium enrichment, the WEC has set in motion a mechanism for such cooperation in a framework of assured supply, geographic dispersion and control against proliferation. The ECG has under discussion draft principles including two related to proliferation and security considerations. The Energy Coordinating Group is not limited to a select group of countries and might serve as a forum for addressing questions relating to the appropriate control on the transfer of technology and equipment.

U.S. Export Controls

Control of export of nuclear technology from the U.S. is based upon provisions of the Atomic Energy Act, the Export Administration Act and the Mutual Security Act. Restricted Data can be communicated to other countries only under stipulated conditions. An Agreement for Cooperation is required and such agreements require Presidential approval and must be submitted to Congress.

Present U.S. export controls over nuclear and nuclear related unclassified equipment, technology and materials are administered by three agencies; (1) AEC, (2) Department of Commerce, and (3) State Department.

Under the Atomic Energy Act of 1954, as amended, authorizations are required from the AEC for the export of byproduct, source, and special nuclear material (SNM), and production and utilization facilities. Licenses for the export of SNM and production and utilization facilities can only be issued by the AEC if the export is undertaken pursuant to an Intergovernmental agreement for cooperation between the U.S. and the recipient country contemplating such exports. These agreements must be approved by the President and submitted for review to the JCAE. Under Part 110 of the AEC's regulations, a specific authorization is required from the Commission for any U.S. person or company to engage in activities outside of the U.S. pertaining to designing, constructing, fabricating, furnishing or operating facilities and equipment related to the chemical processing of irradiated SNM, the production of heavy water, and the separation of isotopes of uranium. The effect of this general authorization is to permit, without specific licensing, the export to non-communist destinations of civilian land-based nuclear reactor technology.

The Commerce Department exercises export controls for the AEC over certain identified nuclear related equipment, material and technology, the majority of which are of a multipurpose nature, that could be utilized in either nuclear or nonnuclear applications. Items controlled by Commerce either for or at the request of the AEC are specifically identified on an "AEC Referral List" which is furnished by the AEC to the Office of Export

Administration (OEA), U.S. Department of Commerce. Any applications received by OEA for export of any of these items are referred to AEC for comment before action is taken on the license. There are approximately 100 items, on the AEC referral list. Many are COCOM controlled items, while some are subject only to U.S. unilateral export control, i.e., they are not controlled internationally by COCOM.

The Office of Munitions Control of the Department of State exercises export controls over (1) naval nuclear propulsion plants, their land prototypes and special facilities for their construction, support, and maintenance including any machinery, device, component, or equipment specifically developed or designed for use in such plants or facilities, as well as technical data relating thereto; (2) any article, material, equipment, or device specially designed or modified for use in the design, development or fabrication of nuclear weapons or nuclear explosive devices, or for use in the devising, carrying out, or evaluating of nuclear weapon tests or any other nuclear explosions; and (3) certain other specially designed items of a nuclear-related nature.

Strengths and Weaknesses of Present Procedures

The foregoing summary reveals that there are a number of existing agreements and understandings to control the export of various materials, equipment and technology. Each of these has limitations in terms of the number and kinds of goods covered, their membership or the destination of exports covered. The fundamental problem is whether major supplier countries desire to join with the U.S. in controlling exports of certain specified commodities in the interest of limiting or retarding the spread of nuclear weapon capabilities. Any curtailment of normal commerce in non-munitions commodities has been strongly resisted by our NATO allies which represent many of the major nuclear supplying countries of the world. This resistance to limiting exports is well documented in our negotiations over the years in COCOM, to limit exports of strategic commodities to Communist bloc countries, and in the Zangger Committee which was established to implement Article III.2.(b) of the Non-Proliferation Treaty. The Zangger Committee experience to date indicates quite clearly that the Europeans would be reluctant to take actions which would limit the economic benefits to their countries. Therefore, the major obstacle facing any agreement among nations to control export throughout the world is not the question of whether adequate export control procedures exist or can be promulgated, but whether major supplying countries can be convinced that some loss of exports is of a higher interest to their well being than the continued promotion of export sales.

D. CONCLUSIONS AND RECOMMENDATIONS

As indicated in the options of Section B, there is a spectrum of forms which a convention might take, and the options discussed are intended to illustrate a range of possibilities rather than specific choices.

Since a convention with specific, rigorous, mandatory, and enforceable provisions appears unlikely to be ratified by many of the most important countries, we believe that the prospects for obtaining effective physical security measures must rest largely on a supplier's understanding. It must be clearly recognized, however, that such an understanding is far from assured and that it will require the cooperation of several countries, most notably France, whose attitude toward such an understanding may be negative.

The bilateral consultations which the President has approved in NSDM-255 and which are now under way may provide some initial indications of the likely attitude of supplier nations toward an agreement of this kind. Before any steps are taken to negotiate an international convention, it is recommended that the two-stage approach described in Options 2 and 4 herein be discussed with the U.K., Canada, the FRG, France and the Soviet Union on a highly confidential basis. The approach is as follows:

a. an international convention by which a large number of countries would subscribe, at least in principle, to adequate and effective physical security standards and procedures which conform to the extent practicable with specific international guidelines. This would be combined with provisions defining international procedures for pursuit, recovery, extradition and prosecution in the event of nuclear theft or sabotage of nuclear facilities.

b. adoption of common policies by the key suppliers to implement and enforce the convention through their bilateral assistance agreements with recipients.

If these countries favor this approach, these consultations might be broadened to include other suppliers including EURATOM, EURODIF, and South Africa.* The initial steps to negotiate a convention might be taken at some point during these consultations, but we believe that this decision should be deferred until the reaction of some of the suppliers is known. It is of course essential that every possible precaution be taken to ensure the confidentiality of consultations among suppliers until the convention is in force.

We strongly favor the UN as the appropriate forum for preparing a convention, and the IAEA as the appropriate forum in which to draft and negotiate the

---

*Alternatively, consultations with supplier nations could take place at the suppliers conference proposed by Secretary Kissinger in the State Department Analytical Staff Meeting.

convention. Other international bodies such as the Zangger Committee and Interpol might be utilized for negotiation or implementation of some components of the convention. Discussions with the UN and the IAEA regarding their possible roles in formulating and verifying compliance with the convention, and as the forum for its negotiation, will of course be necessary before the U.S. proposes a convention. However, if the U.S. opts for a two-stage approach involving a subsequent suppliers' agreement, discussion of the IAEA's possible role in implementing such an agreement should be deferred until the convention has been concluded.

An international convention will require considerable time to bring into effect. There are many steps that could and should be taken to flushout this framework. An action plan might include:

-- An appeal for international action on physical security by the Secretary of State in UNGA;

-- An UNGA resolution agreeing, in principle, to the need for physical security measures and assigning follow-on action to the IAEA if it appears as a result of the above consultations that it would be useful to do so.

-- Consultations with key suppliers to discuss common non-proliferation policies in such areas as technology transfer, additional special arrangements, etc. This could include discussion of some initial common policies on physical security. This might also provide an opportunity to discuss on a confidential basis with other key suppliers the two-step concept and the eventual imposition of specific physical security obligations by the suppliers;

-- Drafting of a convention by IAEA, and multilateral cooperation to bring it into force;

-- Agreement among the suppliers to implement the convention via bilateral supply contracts;

In negotiating a convention, the U.S. tactic should be to advocate a fairly "hard" convention initially, but be prepared to move toward softer provisions as required. Since we believe that a supplier's understanding is a more likely means of achieving rigorous enforcement than an international convention, our objective should be to achieve wide international acceptance of the convention on the hardest terms which will permit that result.

While intelligence liaison channels may assist in exchanges of information related to thefts, or recovery of nuclear materials, the nature and location of the crisis, information required and extent of action to be taken would determine whether intelligence liaison channels should be employed.

Current international agreements on the control of exports provide some information on transfers as well as the embargo of strategic materials. These agreements, such as the Zangger Committee, offer an opportunity to expand the exchange of information and controls.

Form AEC-8
(1-67)
AECM 0240

A

INCOMING AND SIGNATURE TAB

Use this side of the sheet to precede the incoming material when assembling correspondence.

(USE REVERSE SIDE FOR SIGNATURE TAB)

16—75922-4 GPO

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

SECRET/GDS June 3, 1974

National Security Decision Memorandum 255

TO: The Secretary of Defense
The Deputy Secretary of State
The Director, Arms Control and Disarmament Agency
The Director of Central Intelligence
The Chairman, Atomic Energy Commission

SUBJECT: Security and Other Aspects of the Growth and Dissemination of Nuclear Power Industries

The President has reviewed the report of the NSC Under Secretaries Committee (USC), prepared in response to NSDM 235 and forwarded by the USC Chairman on April 5, 1974, outlining steps the United States could take with other nations concerning the problems associated with the increased availability of weapons useable materials from the growth and dissemination of nuclear power industries.

The President has approved the recommended consultations with other countries—particularly present or potential suppliers of materials, technology and equipment—with the objectives detailed in the USC report.

The initial consultations should emphasize but not necessarily be limited to the need for:(1) establishing agreed international guidelines, preferably based on U.S. practice, to ensure the physical security of weapons useable and highly toxic materials whether internationally transferred or indigenously produced; (2) reaching some common principles regarding the supply of sensitive enrichment technology or equipment; (3) avoiding or applying stricter terms for supply in situations where special hazards could be present; and (4) encouraging, where appropriate, multinational enrichment, fuel fabrication and reprocessing facilities.

The Department of State, in coordination with the Atomic Energy Commission (and other interested agencies when appropriate), will have primary responsibility for the conduct of these consultations and for reporting significant developments.

In addition, the President has directed that a prompt study of possible provisions for an international convention concerned with physical security

SECRET/GDS

05265

guidelines be conducted by an Ad Hoc Group, chaired by a representative of the Atomic Energy Commission and comprising representatives of the addressees. In addition, the Ad Hoc Group should explore the idea of establishing better information exchange internationally on transfers of materials, equipment, or technology. The Ad Hoc Group's study should be forwarded by August 12, 1974 for the President's consideration.

Henry A. Kissinger

cc: Chairman, Joint Chiefs of Staff

Form AEC-8
(1-67)
AECM 0240

INCOMING AND SIGNATURE TAB

Use this side of the sheet to precede the signature page when assembling correspondence.

(USE REVERSE SIDE FOR INCOMING TAB)

16—75922-4 GPO

B

PART 73

PHYSICAL PROTECTION OF PLANTS AND MATERIALS

(As republished 12/28/73, unless otherwise indicated)

GENERAL PROVISIONS

§ 73.1 Purpose and scope.

(a) *Purpose.* This part prescribes requirements for physical protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used, for the purpose of protection against acts of industrial sabotage and protection of special nuclear material against theft by establishment and maintenance of a physical protection system of: (1) Protective barriers and intrusion detection devices at fixed sites to provide early detection of an attack, (2) deterrence to attack by means of armed guards and escorts, and (3) liaison and communication with law enforcement authorities capable of rendering assistance to counter such attacks.

(b) *Scope.* (1) This part prescribes requirements for (i) the physical protection of production and utilization facilities licensed pursuant to Part 50 of this chapter; (ii) the physical protection of plants in which activities licensed pursuant to Part 70 of this chapter are conducted, and the physical protection of special nuclear material, by any person who pursuant to the regulations in Part 70 of this chapter possesses or uses at any site or contiguous sites subject to control by the licensee, uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium alone or in any combination in a quantity of 5,000 grams or more computed by the formula, grams=(grams contained U-235)+2.5 *(grams U-233+grams plutonium).

(2) This part prescribes requirements for the physical protection of special nuclear material in transportation by any person who is licensed pursuant to the regulations in Part 70 of this chapter who imports, exports, transports, delivers to a carrier for transport in a single shipment, or takes delivery of a single shipment free on board at the point where it is delivered to a carrier, either uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium, or any combination of these materials, which is 5,000 grams or more computed by the formula, grams=(grams contained U-235)+2.5 (grams U-233+grams plutonium).

(3) This part also applies to shipments by air of special nuclear material in quantities exceeding (i) 20 grams or 20 curies, whichever is less, of plutonium or uranium-233, or (ii) 350 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope).

(4) Special nuclear material subject to this part may also be protected pursuant to security procedures prescribed by the Commission or another Government agency for the protection of classified materials. The provisions and requirements of this part are in addition to, and not in substitution for, any such security procedures. Compliance with the requirements of this part does not relieve any licensee from any requirement or obligation to protect special nuclear material pursuant to security procedures prescribed by the Commission or other Government agency for the protection of classified materials.

§ 73.2 Definitions.

As used in this part:

(a) Terms defined in Parts 50 and 70 of this chapter have the same meaning when used in this part.

(b) "Authorized individual" means any individual, including an employee, a consultant, or an agent of a licensee, who has been designated in writing by a licensee to have responsibility for surveillance of special nuclear material.

(c) "Guard" means a uniformed individual armed with a firearm whose primary duty is the protection of special nuclear material against theft and/or the protection of a plant against industrial sabotage.

(d) "Watchman" means an individual, not necessarily uniformed or armed with a firearm, who provides protection for a plant and the special nuclear material therein in the course of performing other duties.

(e) "Continuous visual surveillance" means unobstructed view at all times of a shipment of special nuclear material, and of all access to a temporary storage

*Corrected

area or cargo compartment containing the shipment.

(f) "Physical barrier" means

(1) Fences constructed of No. 11 American wire gauge, or heavier wire fabric, topped by three strands or more of barbed wire or similar material on brackets angled outward between 30° and 45° from the vertical, with an overall height of not less than eight feet, including the barbed topping.

(2) Building walls constructed of stone, brick, cinder block, concrete, steel or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping described in paragraph (f)(1) of this section of a height of not less than 8 feet.

(3) Ceilings and floors constructed to offer resistance to penetration equivalent to that of building walls described in paragraph (f)(2) of this section.

(g) "Protected area" means an area encompassed by physical barriers and to which access is controlled.

(h) "Vital area" means any area which contains vital equipment within a structure, the walls, roof, and floor of which constitute physical barriers of construction at least as substantial as walls as described in paragraph (f)(2) of this section.

(i) "Vital equipment" means any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

(j) "Material access area" means any location which contains special nuclear material, within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier.

(k) "Isolation zone" means any area, clear of all objects which could conceal or shield an individual, adjacent to a physical barrier, which is monitored to detect the presence of individuals or vehicles within that area.

(l) "Intrusion alarm" means a tamper indicating electrical, electromechanical, electrooptical, electronic or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals.

(m) "Lock" in the case of vaults or vault type rooms means a three-position, manipulation resistant, dial type, built-in combination lock or combination padlock and in the case of fences, walls, and buildings means an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock. "Lock" in the case of a vault or vault type room also means any manipulation resistant, electromechanical device which provides the same function as a built-in combination lock or combination padlock, which can be operated remotely or by the "reading" or insertion of information, which can be uniquely characterized, and which allows operation of the device. "Locked" means protected by an operable lock.

(n) "Vault" means a burglar-resistant windowless enclosure with walls, floor and roof of: (1) Steel at least one-half inch thick, (2) reinforced concrete or stone at least 8 inches thick, (3) non-reinforced concrete or stone at least 12 inches thick, or (4) monolithic floor or roof construction of equivalent resistance to entry, with a built-in lock in a steel door at least 1 inch thick, exclusive of the locking mechanism.

(o) "Vault-type room" means a room with one or more doors, all capable of being locked, protected by an intrusion alarm which creates an alarm upon the entry of a person anywhere into the room and upon exit from the room or upon movement of an individual within the room.

(p) "Industrial sabotage" means any deliberate act directed against a plant in which an activity licensed pursuant to the regulations in this chapter is conducted, or to any component of such a plant, which could directly or indirectly endanger the public health and safety by exposure to radiation, other than such acts by an enemy of the United States, whether foreign government or other person.

§ 73.3 Interpretations.

Except as specifically authorized by the Commission in writing, no interpretation of the meaning of the regulations in this part by any officer or employee of the Commission other than a written interpretation by the General Counsel will be recognized as binding upon the Commission.

§ 73.4 Communications.

Except where otherwise specified, all communications and reports concerning the regulations in this part should be addressed to the Director of Licensing, U.S. Atomic Energy Commission, Washington, D.C. 20545, or may be delivered in person at the Commission's offices at 1717 H Street, NW., Washington, D.C.; at 7920 Norfolk Avenue, Bethesda, Maryland; or at Germantown, Maryland.

§ 73.5 Specific exemptions.

The Commission may, upon application of any interested person or upon its own initiative, grant such exemptions from the requirements of the regulations in this part as it determines are authorized by law and will not endanger life or property or the common defense and security, and are otherwise in the public interest.

§ 73.6 Exemptions for certain quantities and kinds of special nuclear material.

A licensee is exempt from the requirements of §§ 73.30 through 73.36 and of §§ 73.60 and 73.70 of this part, with respect to the following special nuclear material:

(a) Uranium-235 contained in uranium enriched to less than 20 percent in the U-235 isotope:

(b) Special nuclear material which is not readily separable from other radioactive material and which has a total external radiation dose rate in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding; and

(c) Special nuclear material in a quantity not exceeding 350 grams of uranium-235, uranium-233, plutonium, or a combination thereof, possessed in any analytical, research, quality control, metallurgical or electronic laboratory.

PHYSICAL PROTECTION OF SPECIAL NUCLEAR MATERIAL IN TRANSIT

§ 73.30 General requirements.

(a) Except as specified in § 73.36(a) or as otherwise authorized pursuant to § 73.30(f), each licensee who transports or who delivers to a carrier for transport either uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium, or any combination of these materials, which is 5,000 grams or more computed by the formula, grams=(grams contained U-235)+2.5 (grams U-233+grams plutonium), shall make arrangements to assure that such special nuclear material will, if a common or contract carrier is used, be transported under the established procedures of a carrier which provides a system for the physical protection of valuable material in transit and requires an exchange of hand-to-hand receipts at origin and destination and at all points enroute where there is a transfer of custody.

(b) Transit times of shipments other than those specified in § 73.1(b)(3) shall be minimized and routes shall be selected to avoid areas of natural disaster or civil disorders. Such shipments shall be preplanned to assure that deliveries occur at a time when the receiver at the final delivery point is present to accept receipt of shipment.

(c) Special nuclear material shall be shipped in containers which are sealed by tamper indicating type seals. The container shall also be locked if it is not in another container or vehicle which is locked. If inspection of the container or vehicle is not required by State or local authorities before final destination, the outermost container or vehicle shall also be sealed by tamper indicating type seals. No container weighing 500 pounds or less shall be shipped in open trucks, railroad flat cars or box cars and ships. This paragraph does not apply to shipments of quantities specified in § 73.1(b)(3).

(d) When guards are used pursuant to §§ 73.31(c)(1), 73.31(c)(2), 73.33 and 73.35, the licensee shall not permit an individual to act as a guard unless there is documentation that the individual has been qualified by demonstrating an understanding of his duties and responsibilities. The licensee or his agent shall have documentation that guards have been requalified annually.

(e) By January 7, 1974, each licensee shall submit a plan outlining the procedures that will be used to meet the requirements of §§ 73.30 through 73.36 and 73.70(g) including a plan for the selection, qualification, and training of armed escorts, or the specification and design of a specially designed truck or trailer as appropriate. This plan shall be followed by the licensee after March 6, 1974.

(f) A licensee or applicant for a license may apply to the Commission for approval of proposed procedures for transport of special nuclear material in a manner not otherwise authorized by the regulations of this part. Such application shall include a description and quantity of the special nuclear material involved, the origin and destination, the carriers to be used, the expected time in transit, the number of transfer points, the communications to be used, the vehicle visual identification, and the cargo security and surveillance measures to be used.

(g) Paragraphs (b), (c), (d), and (f) of this section are effective March 6, 1974.

§ 73.31 Shipment by road.

(a) All shipments by road shall be made without any scheduled intermediate stops to transfer special nuclear material or other cargo between the facility from which it is shipped and the facility of the receiver.

(b) All motor vehicles used to transport special nuclear material shall be equipped with a radiotelephone which can communicate with a licensee or his agent. The licensee or agent with whom communications shall be maintained for different segments of the shipment shall be predesignated before a shipment is made. Calls to such licensee or agent shall be made at least every 2 hours when radiotelephone or conventional telephone coverage is not available along the preplanned route, at which time a conventional telephone call shall be made. In the event no call is received in accordance with these requirements, the licensee or his agent shall immediately notify an appropriate law enforcement authority and the appropriate Atomic Energy Commission Regulatory Operations Regional Office listed in Appendix A of this part.

(c) A shipment shall be accompanied by at least two people in the vehicle containing the shipment, which may be two drivers or one driver and an authorized individual. The vehicle containing the shipment shall be under continuous visual surveillance, or one of the drivers or authorized individuals shall be in the cab of the vehicle, awake, and not in a sleeper berth. The shipment shall be further protected by one of the following methods:

(1) An armed escort consisting of at least two guards shall accompany the shipment in a separate escort vehicle. Escorts shall maintain continuous vigilance for the presence of conditions or situations which might threaten the security of the shipment, take such action as cir-

cumstances might require to avoid interference with continuous safe passage of the cargo vehicle, provide assistance to, or summon aid for crew of cargo vehicles in case of emergency, check seals and locks at each stop where time permits, and observe the cargo vehicle and adjacent areas during stops or layovers. Continuous radio communication capability shall be provided between the cargo vehicle and the escort vehicle. Escort vehicles shall also be equipped with a radiotelephone. The licensee may use his own employees as armed escorts or he may use an agent. Only the driver is required in the vehicle containing special nuclear material for shipments involving an average of less than an hour in transportation, if communication is maintained during the course of the shipment with the licensee or agent monitoring the shipment.

(2) The shipment shall be made in a specially designed truck or trailer which reduces the vulnerability to diversion. Design features of the truck or trailer shall permit immobilization of the van and provide barriers or deterrents to physical penetration of the cargo compartment unless armed guards are also used in which case immobilization of the vehicle is not required.

(d) Transfers to and from other modes of transportation shall be in accordance with § 73.35.

(e) Vehicles shall be marked on top with identifying letters or numbers which will permit identification of the vehicle under daylight conditions from the air in clear weather at 1,000 feet above ground level. The same code of letters and numbers as those used on the top shall also be marked on the sides and rear of the vehicle to permit identification from the ground.

(f) This section is effective March 6, 1974.

§ 73.32 Shipment by air.

(a) Except as specifically approved by the Atomic Energy Commission, no shipment of special nuclear material shall be made in passenger aircraft in excess of (1) 20 grams or 20 curies, whichever is less, of plutonium or uranium-233, or (2) 350 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U–235 isotope).

(b) In shipments on cargo aircraft of either uranium-235 (contained in uranium enriched to 20 percent or more in the U–235 isotope), uranium-233 or plutonium, or any combination of these materials which is 5,000 grams or more computed by the formula, grams=(grams contained U–235) + 2.5(grams U–233 + grams plutonium), transfers shall be in accordance with § 73.35. Transfers shall be minimized.

(c) Export shipments shall be escorted by an unarmed authorized individual, who may be a crew member, from the last terminal in the United States until the shipment is unloaded at a foreign terminal. He shall perform monitoring duties at foreign terminals as described in § 73.35.

(d) Paragraph (c) of this section is effective March 6, 1974.

§ 73.33 Shipment by rail.

(a) A shipment by rail shall be escorted by two guards, in the shipment car or an escort car of the train, who shall keep the shipment cars under observation and who shall de[illegible] stops when practicable and time permits to guard the shipment cars under observation, and check car or container locks and seals. Radiotelephone communication shall be maintained with a licensee or his agent to relay position every 2 hours or less, and at scheduled stops in the event that radiotelephone coverage was not available in the last 5 hours before the stop. The licensee or agent with whom communications shall be maintained for different segments of the shipment shall be predesignated before a shipment is made. In the event no call is received in accordance with these requirements, the licensee or his agent shall immediately notify an appropriate law enforcement authority and the appropriate Atomic Energy Commission Regulatory Operations Regional Office listed in Appendix A of this part.

(b) Transfers shall be in accordance with § 73.35.

(c) This section is effective March 6, 1974.

§ 73.34 Shipment by sea.

(a) Shipments shall be made on vessels making the minimum ports of call. Transfers to and from other modes of transportation shall be in accordance with § 73.35. There shall be no scheduled transfers to other ships. At domestic ports of call where other cargo is transferred, the shipments shall be protected in accordance with § 73.35(a).

(b) The shipment shall be placed in a secure compartment which is locked and sealed. Locks and seals shall be periodically inspected in transit, if accessible, by an escort or crew member.

(c) Export shipments shall be escorted by an unarmed authorized individual, who may be a crew member, from the last port in the United States until the shipment is unloaded at a foreign port. He shall perform monitoring duties at foreign ports as described in § 73.35.

(d) Ship-to-shore communications shall be available, and a ship-to-shore contact shall be made every twenty-four hours to relay position information, and the status of the shipment, which shall be determined by a daily inspection where possible. This information shall be sent, as often as it is available, to the licensee or his agent who makes the arrangements for the protection of the shipment.

(e) This section is effective March 6, 1974.

§ 73.35 Transfer of special nuclear material.

All transfers shall be monitored by a guard. An alternate guard shall be designated at all transfer points to substitute, if necessary. Monitoring of special nuclear material transfers shall be conducted as follows:

(a) At scheduled intermediate stops where special nuclear material is not scheduled for transfer, the guard shall observe the opening of the cargo compartment and assure that the shipment is not removed. The guard shall maintain continuous visual surveillance of the cargo compartment. Continuous visual surveillance of the cargo compartment shall be maintained up to the time the vehicle is ready to depart. The guard shall observe the vehicle until it has departed, and shall notify the licensee or his agent of the latest status immediately thereafter.

(b) At points where special nuclear material is transferred from a vehicle to storage, from one vehicle to another, or from storage to a vehicle, the guard shall keep the shipment under continuous visual surveillance by observing the opening of the cargo compartment of the incoming vehicle and assuring that the shipment is complete by checking locks and/or seals. Continuous visual surveillance of a shipment shall be maintained at all times it is in the terminal or in storage. Shipments shall be preplanned in order to avoid storage times in excess of 24 hours. Continuous visual surveillance of the cargo compartment shall be maintained up to the time the vehicle is ready to depart from the terminal. The guard shall observe the vehicle until it has departed, and shall notify the licensee or his agent of the latest status immediately thereafter.

(c) The guard shall be required to immediately notify the carrier and the licensee who made the arrangements for protection of special nuclear material of any deviation from or attempted interference with schedule or routing.

(d) This section is effective March 6, 1974.

§ 73.36 Miscellaneous requirements.

(a) Each licensee who takes delivery of special nuclear material free on board (f.o.b.) the point at which it is delivered to a carrier for transport shall make the arrangements to assure that such special nuclear material will be protected in transit as prescribed in §§ 73.30 through 73.35, rather than the person who delivers such shipment to the carrier for transport.

(b) Each licensee who imports special nuclear material shall make arrangements to assure that such material will be protected in transit as follows:

(1) An individual designated by the licensee or his agent, or as specified by a contract of carriage, shall confirm the container count and examine locks and/or seals for evidence of tampering, at the first place in the United States at which the shipment is discharged from the arriving carrier.

(2) The shipment shall be protected at the first terminal at which it arrives in the United States and all subsequent terminals as provided in §§ 73.30 through 73.35 and paragraphs (c) and (f) of this section.

(c) (1) Each licensee who delivers special nuclear material to a carrier for transport shall immediately notify the consignee by telephone, telegraph, or teletype, of the time of departure of the shipment, and shall notify or confirm with the consignee the method of transportation, including the names of carriers, and the estimated time of arrival of the shipment at its destination. (2) In the case of a shipment free on board (f.o.b.) the point where it is delivered to a carrier for transport, each licensee shall, before the shipment is delivered to the carrier, obtain written certification from the licensee who is to take delivery of the shipment at the f.o.b. point that the physical protection arrangements required by §§ 73.30 through 73.35 for licensed shipments have been made. When an AEC license-exempt contractor is the consignee of a shipment, the licensee shall, before the shipment is delivered to the carrier, obtain written certification from the contractor who is to take delivery of the shipment at the f.o.b. point that the physical protection arrangements required by AEC Manual Chapters 2401 or 2405 have been made. (3) Each licensee who delivers special nuclear material to a carrier for transport shall also make arrangements with the consignee to be notified immediately by telephone, telegraph, or teletype, of the arrival of the shipment at its destination.

(d) In addition to complying with the requirements specified in paragraphs (c) and (f) of this section, each licensee who exports special nuclear material shall comply with the requirements specified in §§ 73.30 through 73.35, as applicable, up to the first point where the shipment is taken off the vehicle outside the United States. The licensee shall also make arrangements with the consignee to be notified immediately by telephone and telegraph, teletype, or cable, of the arrival of the shipment at its destination, or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination.

(e) Each licensee who receives a shipment of special nuclear material shall immediately notify the person who delivered the material to a carrier for transport of the arrival of the shipment at its destination. In the event such a shipment fails to arrive at its destination at the estimated time, the consignee, if a licensee, or in the case of an export shipment, the licensee who exported the shipment, shall immediately notify by telephone and telegraph, or teletype, the Director of the appropriate Atomic Energy Commission Regulatory Operations Regional Office listed in Appendix A of this part, and the licensee or other person who delivered the material to a carrier for transport. The licensee who made the physical protection arrangements shall also immediately notify by telephone and telegraph, or teletype the Director of the appropriate Atomic Energy Commission Regulatory Operations Regional office listed in Appendix A of the action being taken to trace the shipment.

(f) Each licensee who makes arrangements for physical protection of a shipment of special nuclear material as required by §§ 73.30 through 73.36 shall immediately conduct a trace investigation of any shipment that is lost or unaccounted for after the estimated arrival time and file a report with the Commission as specified in § 73.71. If the licensee who conducts the trace investigation is not the consignee, he shall also immediately report the results of his investigation by telephone and telegraph, or teletype to the consignee.

(g) Paragraphs (a), (b), (c) and (d) of this section are effective March 6, 1974.

PHYSICAL PROTECTION REQUIREMENTS AT FIXED SITES

§ 73.40 Physical protection: General requirements at fixed sites.

Each licensee shall provide physical protection against industrial sabotage and against theft of special nuclear material at the fixed sites where licensed activities are conducted. Security plans submitted to the Commission for approval shall be followed by the licensee after March 6, 1974.

§ 7?.50 Requirements for physical protection of licensed activities.

In addition to any other requirements of this part, each licensee who is authorized to operate a fuel reprocessing plant pursuant to Part 50 of this chapter or who possesses or uses uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium alone or in any combination in a quantity of 5000 grams or more computed by the formula, grams = (grams contained U-235) + 2.5 (grams U-233 + grams plutonium), other than in the operation of a nuclear reactor licensed pursuant to Part 50 of this chapter, shall comply with the following.

(a) *Physical security organization.* (1) The licensee shall establish a security organization, including guards, to protect his facility against industrial sabotage and the special nuclear material in his possession against theft.

(2) At least one supervisor of the security organization shall be on site at all times.

(3) The licensee shall establish, maintain and follow written security procedures which document the structure of the security organization and which detail the duties of guards, watchmen, and other individuals responsible for security.

(4) The licensee shall not permit an individual to act as a guard or watchman unless such individual has been properly trained and equipped and has qualified by demonstrating: (i) An understanding of the licensee's security procedures, and (ii) the ability to execute all duties required of him by such procedures. Each guard and watchman shall be requalified at least annually. Such requalification shall be documented.

(b) *Physical barriers.* (1) The licensee shall locate vital equipment only within a vital area, which, in turn, shall be located within a protected area such that access to vital equipment requires passage through at least two physical barriers. More than one vital area may be within a single protected area.

(2) The licensee shall locate material access areas only within protected areas such that access to the material access area requires passage through at least two physical barriers. More than one material access area may be within a single protected area.

(3) The physical barrier at the perimeter of the protected area shall be separated from any other barrier designated as a physical barrier within the protected area, and the intervening space monitored or periodically checked to detect the presence of persons or vehicles so that the facility security organization can respond to suspicious activity or to the breaching of any physical barrier.

(4) An isolation zone shall be maintained around the physical barrier at the perimeter of the protected area and any part of a building used as part of that physical barrier. The isolation zone shall be monitored to detect the presence of individuals or vehicles within the zone so as to allow response by armed members of the licensee security organization to be initiated at the time of penetration of the protected area. Parking facilities, both for employees and visitors, shall be located outside the isolation zone.

(5) Isolation zones and clear areas between barriers shall be provided with illumination sufficient for the monitoring required by paragraph (b) (3) and (4) of this section, but not less than 0.2 foot candles.

(c) *Access requirements.* The licensee shall control all points of personnel and vehicle access into a protected area, including shipping or receiving areas, and into each vital area. Identification of personnel and vehicles shall be made and authorization shall be checked at such points.

(1) At the point of personnel and vehicle access into a protected area, all individuals, except employees who possess an AEC personnel security clearance, and all hand-carried packages shall be searched for devices such as firearms, explosives, and incendiary devices, or other items which could be used for industrial sabotage. The search shall be conducted either by a physical search or by the use of equipment capable of detecting such devices. Employees who possess an AEC personnel security clearance shall be searched at random intervals. Subsequent to search, drivers of delivery and service vehicles shall be escorted at all times while within the protected area.

(2) All packages being delivered into the protected area shall be checked for proper identification and authorization. Packages other than hand-carried packages shall be searched at random intervals.

(3) A picture badge identification system shall be used for all individuals who are authorized access to protected areas without escort.

(4) Access to vital areas and material access areas shall be limited to individuals who are authorized access to vital equipment or special nuclear material

and who require such access to perform their duties. Authorization for such individuals shall be provided by the issuance of specially coded numbered badges indicating vital areas and material access areas to which access is authorized. Unoccupied vital areas and material access areas shall be protected by an active intrusion alarm system.

(5) Individuals not employed by the licensee shall be escorted by a watchman, or other individual designated by the licensee, while in a protected area and shall be badged to indicate that an escort is required. In addition, each individual not employed by the licensee shall be required to register his name, date, time, purpose of visit, employment afiliation, citizenship, name and badge number of the escort, and name of the individual to be visited. Except for a driver of a delivery or service vehicle, an individual not employed by the licensee who requires frequent and extended access to a protected area or a vital area need not be escorted provided such individual is provided with a picture badge, which he must receive upon entrance into the protected area and which he must return each time he leaves the protected area, which indicates (i) nonemployee-no escort required, (ii) areas to which access is authorized, and (iii) the period for which access has been authorized.

(6) No vehicles used primarily for the conveyance of individuals shall be permitted within a protected area except under emergency conditions.

(7) Keys, locks, combinations, and related equipment shall be controlled to minimize the possibility of compromise and promptly changed whenever there is evidence that they have been compromised. Upon termination of employment of any employee, keys, locks, combinations, and related equipment to which that employee had access shall be changed.

(d) *Detection aids.* (1) All alarms required pursuant to this part shall annunciate in a continuously manned central alarm station located within the protected area and in at least one other continuously manned station, not necessarily within the protected area, such that a single act cannot remove the capability of calling for assistance or otherwise responding to an alarm. All alarms shall be self-checking and tamper indicating. The annunciation of an alarm at the onsite central alarm station shall indicate the type of alarm (e.g., intrusion alarm, emergency exit alarm, etc.) and location. All intrusion alarms, emergency exit alarms, alarm systems, and line supervisory systems shall at minimum meet the performance and reliability levels indicated by GSA Interim Federal Specification W-A-00450 B (GSA-FSS).

(2) All emergency exits in each protected area and each vital area shall be alarmed.

(e) *Communication requirements.* (1) Each guard or watchman on duty shall be capable of maintaining continuous communication with an individual in a continuously manned central alarm station within the protected area, who shall be capable of calling for assistance from other guards and watchmen and from local law enforcement authorities.

(2) The alarm stations required by paragraph (d)(1) of this section shall have conventional telephone service for communication with the law enforcement authorities as described in paragraph (e)(1) of this section.

(3) To provide the capability of continuous communication, two-way radio voice communication shall be established in addition to conventional telephone service between local law enforcement authorities and the facility and shall terminate at the facility in a continuously manned central alarm station within the protected area.

(4) All communications equipment, including offsite equipment, shall remain operable from independent power sources in the event of loss of primary power.

(f) *Testing and maintenance.* Each licensee shall test and maintain intrusion alarms, emergency alarms, communications equipment, physical barriers, and other security related devices or equipment utilized pursuant to this section as follows:

(1) All alarms, communications equipment, physical barriers, and other security related devices or equipment shall be maintained in operable and effective condition.

(2) Each intrusion alarm shall be functionally tested for operability and required performance at the beginning and end of each interval during which it is used for security, but not less frequently than once every seven (7) days.

(3) Communications equipment shall be tested for operability and performance not less frequently than once at the beginning of each security personnel work shift.

(g) *Response requirement.* (1) The licensee shall establish liaison with local law enforcement authorities. In developing his physical security plan, the licensee shall take account of the probable size and response time of the local law enforcement authority assistance.

(2) Upon detection of abnormal presence or activity of persons or vehicles within an isolation zone, a protected area, a material access area or a vital area, or upon evidence of intrusion into a protected area, a material access area or a vital area, the facility security organization shall (i) determine whether or not a threat exists, (ii) assess the extent of the threat, if any, and (iii) take immediate measures to neutralize the threat, either by appropriate action by facility guards or by calling for assistance from local law enforcement authorities, or both.

(h) This section is effective March 6, 1974.

§ 73.60 Additional requirements for the physical protection of special nuclear material at fixed sites.

In addition to the applicable requirements of § 73.50, each licensee who pursuant to the regulations in Part 70 of this chapter possesses at any site or contiguous sites subject to control by the licensee uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium alone or in any combination in a quantity of 5,000 grams or more computed by the formula, grams=(grams contained U-235) + 2.5 (grams U-233 + grams plutonium) shall protect the special nuclear material from theft or diversion as follows:

(a) *Access requirements.* (1) Special nuclear material shall be stored or processed only in a material access area. No activities other than those which require access to special nuclear material or equipment employed in the process, use, or storage of special nuclear material, shall be permitted within a material access area.

(2) Material access areas shall be located only within a protected area to which access is controlled.

(3) Special nuclear material not in process shall be stored in a vault equipped with an intrusion alarm or in a vault-type room, and each such vault or vault-type room shall be controlled as a separate material access area.

(4) Enriched uranium scrap in the form of small pieces, cutings, chips, solutions or in other forms which result from a manufacturing process, contained in 30-gallon or larger containers, with a uranium-235 content of less than 0.25 grams per liter, may be stored within a locked and separately fenced area which is within a larger protected area provided that the storage area is no closer than 25 feet to the perimeter of the protected area. The storage area when unoccupied shall be protected by a guard or watchman who shall patrol at intervals not exceeding 4 hours, or by intrusion alarms.

(5) Admittance to a material access area shall be under the control of authorized individuals and limited to individuals who require such access to perform their duties.

(6) Prior to entry into a material access area, packages shall be searched for devices such as firearms, explosives, incendiary devices, or counterfeit substitute items which could be used for theft or diversion of special nuclear material.

(7) Methods to observe individuals within material access areas to assure that special nuclear material is not diverted shall be provided and used on a continuing basis.

(b) *Exit requirement.* Each individual, package, and vehicle shall be searched for concealed special nuclear material before exiting from a material access area unless exit is into a contiguous material access area. The search may be carried out by a physical search or by use of equipment capable of detecting the presence of concealed special nuclear material.

(c) *Detection aid requirement.* Each unoccupied material access area shall be locked and protected by an intrusion alarm on active status. All emergency exits shall be continuously alarmed.

(d) *Testing and maintenance.* Each licensee shall test and maintain intrusion alarms, physical barriers, and other devices utilized pursuant to the requirements of this section as follows:

(1) Intrusion alarms, physical barriers, and other devices used for material protection shall be maintained in operable condition.

(2) Each intrusion alarm shall be inspected and tested for operability and required functional performance at the beginning and end of each interval during which it is used for material protection, but not less frequently than once every seven (7) days.

(e) This section is effective March 6, 1974.

RECORDS AND REPORTS

§ 73.70 Records.

Each licensee subject to the provisions of §§ 73.30 through 73.36 and/or § 73.50 and/or § 73.60 shall keep the following records:

(a) Names and addresses of all individuals who have been designated as authorized individuals.

(b) Names, addresses, and badge numbers of all individuals authorized to have access to vital equipment or special nuclear material, and the vital areas and material access areas to which authorization is granted.

(c) A register of visitors, vendors, and other individuals not employed by the licensee recorded pursuant to § 73.50(c)(5).

(d) A log indicating name, badge number, time of entry, reason for entry, and time of exit of all individuals granted access to a normally unoccupied vital area.

(e) Documentation of all routine security tours and inspections, and of all tests, inspections, and maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security related equipment used pursuant to the requirements of this part.

(f) A record at each onsite alarm annunciation location of each alarm, false alarm, alarm check, and tamper indication that identifies the type of alarm, location, alarm circuit, date, and time. In addition, details of response by facility guards and watchmen to each alarm, intrusion, or other security incident shall be recorded.

(g) Shipments of special nuclear material subject to the requirements of this part, including names of carriers, major roads to be used, flight numbers in the case of air shipments, dates and expected times of departure and arrival of shipments, names and addresses of the monitor and one alternate monitor at each transfer point, verification of communication equipment on board the transfer vehicle, names of individuals who are to communicate with the transport vehicle, container seal descriptions and identification, and any other information to confirm the means utilized to comply with §§ 73.30 through 73.36. Such information shall be recorded prior to shipment. Information obtained during the course of the shipment such as reports of all communications, change of shipping plan including monitor changes, trace investigations and others shall also be recorded.

(h) Procedures for controlling access to protected areas and for controlling access to keys for locks used to protect special nuclear material.

§ 73.71 Reports of unaccounted for shipments, suspected theft, unlawful diversion, or industrial sabotage.

(a) Each licensee who conducts a trace investigation of a lost or unaccounted for shipment pursuant to § 73.36(f) shall immediately report to the Director of the appropriate Atomic Energy Commission Regulatory Operations Regional Office listed in Appendix A, by telephone, telegram, or teletype, the details and results of his trace investigation and shall file within a period of fifteen (15) days a written report to the Director of the appropriate Regulatory Operations Regional Office with a copy to the Director of Regulatory Operations, U.S. Atomic Energy Commission, Washington, D.C. 20545, setting forth the details and results of the trace investigation.

(b) Each licensee shall report immediately to the Director of the appropriate Atomic Energy Commission Regulatory Operations Regional Office listed in Appendix A, by telephone, telegram, or teletype, any incident in which an attempt has been made, or is believed to have been made, to commit a theft or unlawful diversion of special nuclear material which he is licensed to possess, or to commit an act of industrial sabotage against his plant. The initial report shall be followed within a period of fifteen (15) days by a written report submitted to the Director of the appropriate Regulatory Operations Regional Office, with a copy to the Director of Regulatory Operations, U.S. Atomic Energy Commission, Washington, D.C. 20545, setting forth the details of the incident. Subsequent to the submission of the written report required by this paragraph, a licensee shall immediately inform the Director of the appropriate Regulatory Operations Regional Office by means of a written report of any substantive additional information, which becomes available to the licensee, concerning the incident.

ENFORCEMENT

§ 73.80 Violations.

An injunction or other court order may be obtained prohibiting any violation of any provision of the Act or any regulation or order issued thereunder. A court order may be obtained for the payment of a civil penalty imposed pursuant to section 234 of the Act for violation of sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Act or any rule, regulation, or order issued thereunder, or any term, condition, or limitation of any license issued thereunder, or for any violation for which a license may be revoked under section 186 of the Act. Any person who willfully violates any provision of the Act or any regulation or order issued thereunder may be guilty of a crime and upon conviction, may be punished by fine or imprisonment or both, as provided by law.

APPENDIX A

U.S. ATOMIC ENERGY COMMISSION REGULATORY OPERATIONS REGIONAL OFFICES

Region and address	Telephone	
	Daytime	Nights and holidays
Region I, Directorate of Regulatory Operations, USAEC, 631 Park Ave., King of Prussia, Pa. 19406.	215-337-1150	215-337-1150.
Region II, Directorate of Regulatory Operations, USAEC, Suite 818, 230 Peachtree St. NW., Atlanta, Ga. 30303.	404-526-4503	404-526-4503.
Region III, Directorate of Regulatory Operations, USAEC, 799 Roosevelt Rd., Glen Ellyn, Ill. 60137.	312-858-2660	312-739-7711.
Region V, Directorate of Regulatory Operations, USAEC, P.O. Box 1515, Berkeley, Calif. 94701.	*415-486-3141	415-273-4237.

For the purposes of this regulation, the geographical areas assigned to the regional offices are as follows:

REGION I

Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, and Vermont.

REGION II

Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Puerto Rico, South Carolina, Tennessee, Virginia, and West Virginia.

REGION III

Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, Oklahoma, South Dakota, and Wisconsin.

REGION V

Alaska, Arizona, California, Colorado, Hawaii, Idaho, Montana, Nevada, New Mexico, Oregon, Texas, Utah, Washington, and Wyoming.

*Amended

June 1973

U.S. ATOMIC ENERGY COMMISSION
REGULATORY GUIDE
DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.7

CONTROL OF PERSONNEL ACCESS TO PROTECTED AREAS, VITAL AREAS, AND MATERIAL ACCESS AREAS

A. INTRODUCTION

Proposed amendments to the Commission regulations of 10 CFR Part 50, "Licensing of Production and Utilization Facilities," 10 CFR Part 70, "Special Nuclear Material," and 10 CFR Part 73, "Physical Protection of Special Nuclear Material," would, if adopted, require measures (1) for the protection against industrial sabotage of fuel reprocessing plants and certain facilities subject to the provisions of 10 CFR Part 70 and (2) for the protection of special nuclear material (SNM) against theft or diversion from certain licensed facilities.

One element of this protection is proper control of access of personnel to and from protected areas, vital areas, and material access areas. Searching persons and packages for firearms, explosives, and other devices which could aid in sabotage or theft of SNM is another element of physical protection.

This guide describes acceptable methods of searching personnel prior to entry into a protected area and upon exit from a material access area, and of controlling access to protected areas, vital areas, and material access areas.

B. DISCUSSION

The objective of controlling access to protected areas, vital areas, and material access areas is to ensure that (1) only persons authorized access to a protected area are permitted within that area and (2) that only individuals authorized access to vital equipment or special nuclear material will be allowed within vital areas or material access areas.

The objective of searching individuals prior to permitting entry into a protected area is to prevent illicit passage into the protected area of objects such as firearms, explosives, and incendiary devices which could aid in industrial sabotage to the facility or in the theft of special nuclear material. Searching individuals and packages for concealed special nuclear material at exit points from material access areas provides a means of detecting attempted theft or diversion of special nuclear material.

Some means by which control of access can be accomplished include a key and lock system, a magnetic or electronic key-card system, an attendant guard or watchman, or a closed-circuit TV (CCTV) in conjunction with keys or key-cards. Of these means, the magnetic or electronic key-card system in conjunction with closed-circuit TV offers the greatest security with a minimum of personnel. The key-cards are much more difficult to duplicate than keys and the locks cannot be "picked." Further, the control system can "read" the key-card and record the identity of the card (to whom it was issued) and the time of entry. A closed-circuit TV system would allow visual observation of the access point without requiring an attendant guard or watchman. In fact, by use of closed-circuit TV several such access points can be maintained under observation by a single guard or watchman. Such a system would be especially useful at access points to remote or normally unoccupied vital areas or material access areas. In any case, visual observation, either directly or via CCTV, provides a positive means of assuring that only individuals authorized access to an area pass through the access point into the area.

Searching of individuals can be carried out by means of a hands-on search ("frisking"), or by means of devices which will detect the presence of weapons and explosives or SNM concealed on the individual, or by a combination of both. The search should be conducted in a manner which (1) provides assurance that firearms, explosives, and other such contraband are not being carried into the protected area and that SNM is not being transported out of a material access area and (2) minimizes inconvenience to the individuals being searched. The use of equipment capable of detecting weapons, explosives, or SNM is usually the preferable form of searching, since the use of detection devices avoids the personal imposition of a hands-on search.

An "airport type" weapon (metal) detector located in a passageway arranged so that all individuals entering the protected area pass through the detector provides a convenient and effective means of searching for firearms.

Devices capable of detecting dynamite, TNT, and other explosives can be used to search individuals for concealed explosives. Most explosive detectors commercially available at present are of the hand-held "sniffer" variety; hence an attendant guard or watchman must pass the detector over the individual being searched. However, it is possible to locate an explosive detector in a passageway and to use the detector in the same manner that a fixed weapon detector is used.

If a hand-held explosive detector is used, the explosive check is best made after the weapon detector has indicated that no weapon is concealed upon the individual. This procedure affords greater protection to the attendant guard or watchman on the presumption that concealed explosives offer less of an immediate danger to the guard or watchman than a concealed firearm.

One alternative approach to the hand-held explosive detector would be the location of an explosive detector within a revolving-door frame. The rather small volume of air trapped in a section of the revolving door would be sampled by the explosive detector and, as the isolation of the air volume by a revolving door section provides some concentration of vapors emitted by any explosives within that section, the effectiveness of the detector would be increased. To further increase efficiency of the explosive detector, the air in the door section might be flushed through the detector.

Searching individuals for concealed SNM upon exit from material access areas can be accomplished in a variety of ways. For example, at facilities processing plutonium or uranium-233 the search for concealed SNM can be made in an attended air lock between change rooms. At areas where only highly enriched uranium is processed, the search can be carried out by use of a doorway SNM monitor and a metal detector in conjunction with a closed-circuit TV (CCTV) system, hence a guard or watchman need not be attendant. However, whether or not the access point is attended, the use of both an SNM monitor and a metal detector would seem necessary to assure that enriched uranium, shielded or unshielded, is not being concealed. In addition, exit from any material access area should be controlled to assure that all individuals and packages exiting from a material access area pass through the SNM check system.

It is the facility guards and watchmen who are charged with the responsibility of assuring that firearms, explosives, and other similar items or devices are not transported into the protected area and that SNM is not removed from a material access area without authorization. Hence, they should search any packages being carried into the protected area or out of a material access area. No individual should be allowed to directly hand carry any package, valise, tool box, or similar hand-carriable item into the protected area or out of a material access area. Such objects should be handed to an attendant guard or watchman who will check them and pass them into the protected area or out of the material access area. To further reduce the possibility of concealment, where feasible, bulky outer clothing such as overcoats, raincoats, greatcoats, and ski jackets should be left in a cloak room provided outside the protected area and in any case should never be taken into a material access area. The licensee may wish to use several members of the security force to check packages, coats, etc., during shift change to minimize the delay encountered in gaining access. Unattended access points into the protected area can be used, provided observation of such points is maintained by CCTV to assure that packages are not being hand carried into the protected area at that point.

Posting of a sign in a conspicuous location will inform individuals requesting access into the protected area that they will be searched, and that any packages, etc., they wish to take into the protected area will also be searched.

Although the Commission regulations do not require searching of individuals entering a material access area, observation of access points provides a convenient method of ensuring that personnel do not carry weapons, explosives, and other similar items or devices into the material access area.

In emergency situations, such as those which may require the evacuation of a material access area, the objectives of access control and search should not be allowed to compromise health and safety. Hence, the licensee should develop plans of action and provide areas and equipment for searching and controlling access under emergency conditions compatible with the objectives of both safety and security. Such emergency procedures will minimize the effectiveness of an emergency situation deliberately perpetrated to conceal theft of SNM.

Administrative controls, as well as physical barriers where applicable, may be employed to gather evacuating individuals within a holding area. Such controls would serve both to verify that no one has remained in the evacuated area and to ensure that an emergency situation will not successfully conceal an attempted theft of SNM.

C. DEFINITIONS

For the purpose of this guide the following definitions are provided:

1. "Guard" means an armed and uniformed individual whose primary duty is the protection of materials and property to the extent that theft of SNM or sabotage of the facility could pose a threat to the common defense and security or result in a radiological hazard to public health and safety.

2. "Watchman" means an unarmed individual, not necessarily uniformed, who provides protection for materials and property in the course of performing other duties.

3. "Patrol watchman" means an arms-qualified individual whose primary duty, at least during threat or emergency situations, is the protection of material and property, and who is normally unarmed but who may be armed during emergency or threat situations. A patrol watchman may or may not be uniformed.

D. REGULATORY POSITION

1. Protected Areas

a. Identity and Authorization

At each access point into a protected area, an identity and access authorization check should be made in conjunction with a search for firearms and explosives. Such identity and access authorization checks should be performed by an attendant guard or watchman or by means of an electronic or magnetic key-card system and a closed-circuit TV system. Packages should be taken into the protected area only at access points attended by a guard or watchman. If the access point is unattended, the individual monitoring the access point via closed-circuit TV should carefully observe any individual requesting access at that point to ensure that no packages are being carried into the protected area.

b. Personnel Search

If the search of individuals is to be carried out by means of detection equipment, a weapon (metal) detector and an explosive detector should be used. An acceptable arrangement for the use of detection equipment in a secure access passageway is illustrated in Figure 1. The doors on the secure access passageway should be interlocked so that both cannot be simultaneously open, thus providing positive access control. An explicit enabling act should be required of a security individual, either attending the secure access passageway or in the central alarm station, to open the inner door.

c. Metal Detector

The metal detector located within the secure access passageway should be capable of detecting a minimum of 200 grams of non-ferrous metal placed anywhere on the body at a 90% confidence limit. The false alarm rate should be a maximum of 1%.

d. Explosive Detector

The explosive detector, as a minimum, hould be capable of detecting dynamite, TNT, and similar nitrogen compounds in minimum amounts of 200 grams at a 90% confidence limit. The false alarm rate should be a maximum of 1%. If detector is hand held rather than permanently fixed to a passageway or revolving door frame, hence requiring an attendant guard or watchman, the search for explosives should be performed after the search for firearms. An acceptable arrangement is illustrated in Figure 2.

e. Alarm Annunciation

The alarms of the weapon detector and the explosive detector should annunciate at the location of the detectors, if attended, as well as in a central alarm station. The alarm annunciation at the location of the detectors need not be aural.

f. Alarm System

The alarms of the weapon (metal) detector and the explosive detector should be interfaced with the inner door lock so that, with an alarm triggered, the inner door cannot be opened from either side without a specific action by the individual manning the central alarm station acknowledging the alarm and enabling the inner door to be opened.

2. Material Access Areas Containing Pu or U-233

a. Change Room Exit

Checking for concealed plutonium or uranium-233 at an exit point from a material access area into a protected area should be performed in an attended secure access passageway located between change rooms. An acceptable arrangement is shown in Figure 3. Unless exit is into a contiguous material access area, all individuals should exit from material access area, other than a vault, only via the change rooms and should be required to deposit all work clothing in the inner change room, walk through the passageway, and dress in street clothing in the outer change room. The licensee should generally not allow packages to be transported out of the material access area via the change rooms. Showers, except those used exclusively for health physics, should be located in the outer change room. A guard or watchman need not be attendant except when personnel are exiting from the material access area.

b. SNM Detector

An SNM detector should be located within the passageway. The detector should be capable of detecting 0.5 gram of plutonium or 1 gram of uranium-233 shielded by 3 mm of brass concealed anywhere on an individual at a 90% confidence limit. The false alarm rate on the detector should be less than 0.1%.

c. **Door Interlock**

The doors of the attended secure access passageway should be interlocked so that both cannot be simultaneously open. The doors should also be alarmed so that an explicit action must be taken by either the attendant security individual or the individual manning the central alarm station to enable either door to open without triggering the alarm.

d. **Packages**

All packages, including waste barrels and work clothes hampers, being transported out of a material access area should be checked by an attendant guard or watchman for concealed SNM, preferably at an exit point expressly provided for packages. SNM packages should be checked for proper seals, identification, and transfer documentation.

e. **Change Room Access**

Access by personnel into a material access area should be permitted only through the change rooms. Control of access should be accomplished either by a guard or watchman attending the secure access passageway between the change rooms, or by a combination of key-card and CCTV when the passageway is unattended.

f. **Observation of Individuals**

Procedures should be employed in the control of access to material access areas to ensure that no lone individual is allowed within a material access area without some means to observe that individual's activities.

3. **Material Access Areas Containing Highly Enriched Uranium, and Vaults Containing SNM**

a. **Exit**

At material access area exit points, the check for concealed SNM should be carried out by means of an SNM doorway monitor and a metal detector. A secure access passageway located at the exit point from the material access area should house the detection equipment. An attendant guard or watchman or a closed-circuit TV connected to the central alarm station should also be provided. Administrative procedures should require the passage of packages only through attended exit points. The doors of the secure access passageway should be interlocked so that both cannot be simultaneously open. A suggested layout is illustrated in Figure 4.

b. **SNM Detector**

The SNM doorway monitor in the secure access passageway should be capable of detecting a minimum of 3 grams uranium enriched to 90% in the uranium-235 isotope in 3 mm of brass concealed anywhere on an individual at a 50% confidence limit. The false alarm rate should not exceed 0.1%.

c. **Metal Detector**

The metal detector in the secure access passageway should be capable of detecting a minimum of 100 grams of non-ferrous metal (shielding) at a 90% confidence limit concealed anywhere on an individual. The false alarm rate should not exceed 0.1%.

d. **Alarms**

The doors of the secure access passageway should be alarmed and interfaced with the doorway monitor such that an individual can be detained for a sufficient time for the doorway monitor to operate. If an individual passes through without waiting for the proper period of time (perhaps indicated by a light) the alarm should sound. The doorway monitor and metal detector alarms and the door alarms should annunciate in the central alarm station and may also annunciate at the passageway.

e. **Access**

The exit points from the material access area should be used for access points as well. Control of access should be by either the attendant security individual or by a key-card CCTV system.

f. **Closed-Circuit TV Observation**

If observation of the passageway is accomplished by CCTV, the guard or watchman monitoring the passageway should carefully observe any individual within to ensure that no packages are being carried into or out of the access area.

g. **Observation of Individuals**

Procedures should be employed in the control of access to material access areas to ensure that no lone individual is allowed within a material access area without some means to observe that individual's activities.

h. **Vaults**

A key-card CCTV system should be employed to control access to and from a vault if such access and exit points do not open to or from material access areas contiguous to the vault. In addition, all individuals who transport SNM between material access areas or to or from a vault, should be escorted by a member of the facility's security force during any period of the transport that the SNM is not within a material access area.

4. **Vital Areas**

Control of access into vital areas should be accomplished either by an attendant guard or watchman, or by means of magnetic or electronic key-card access in conjunction with closed-circuit TV. The identification check should include either direct observation by an attendant guard or watchman or observation by CCTV of each individual passing into the vital area, or some alternate means (e.g., an escort) which will provide positive assurance that only individuals authorized access to the vital area are permitted to pass into that area.

5. Security Force Response to an Alarm

The guards and patrol watchmen should be trained and prepared to protect the facility from sabotage and the SNM within from theft.

a. Protected Area Access Point

Upon annunciation of an alarm from explosive or weapon detection equipment located at a protected area access point attended by a lone guard or watchman, a guard should be dispatched immediately to the access point originating the alarm. If the access point is unattended, two guards should be sent to the access point. At the access point the guard or watchman should request that the individual's pockets be emptied and that the individual pass again through the detection equipment. If the individual complies and if the alarms do not register, the individual may be allowed to pass into the protected area after the contents of the individual's pockets have been examined verifying that no attempt has been made to pass explosives or firearms into the protected area. If, however, an alarm continues to register, the individual should be physically searched by an *unarmed* security individual, while at least one guard or armed patrol watchman observes, to verify that no firearms or explosives are yet concealed by the individual. If the individual refuses to comply with the request for further searching, or if a weapon or explosives are found, the individual should be denied access.

b. Material Access Area Exit Point

If an SNM or metal detector alarm or a door alarm is triggered at a material access area exit point attended by a guard or watchman or at an unattended exit point, security personnel, at least one of whom is armed (a guard or armed patrol watchman), should be dispatched to that exit point. The individual should be searched by emptying pockets and passing again through the detection equipment or by a hands-on search performed by an *unarmed* security individual while at least one guard or armed patrol watchman observes. The cause of the alarm should be determined before the individual is released. If the cause of the alarm was an object, metal or SNM, not concealed by the individual, the individual should be searched without the object to ensure that the object is not a decoy and that SNM is not still being concealed by the individual. If the security personnel determine that attempted unauthorized removal of SNM has been made with the intent to steal SNM, local police and the Federal Bureau of Investigation should be contacted, and the individual should be held by the security personnel until the local police arrive and arrest the individual.

c. Unoccupied Vital Areas and Material Access Areas

If unauthorized entry is made or attempted into a vital area or material access area, or if an intrusion alarm protecting an unoccupied vital or material access area is triggered, two armed security personnel should be dispatched immediately to the area of alarm. If, however, the area of the alarm can be observed by CCTV, the guard or watchman in the alarm station where the TV monitor is located should first verify the existence of intrusion and assess the extent of a threat, if any, before dispatching the security personnel. If the existence of an intrusion is verified, either by CCTV or security personnel in the area, a law enforcement authority should be notified immediately. If possible, the intruder(s) found by the security personnel should be searched and detained until arrest by local police.

6. Emergency Procedures

The licensee should provide procedures and equipment to maintain the level of access control and SNM and facility protection during conditions of emergency or equipment failure. Emergency procedures should be developed and executed in a manner consistent with safety.

a. Evacuation Procedures

During emergency conditions which require evacuation of part or all of the facility, temporary SNM checking stations should be established at the perimeter of the protected area or at a personnel collection area outside the protected area. All individuals should be searched for concealed SNM before being released from the protected area or collection area. In addition, a roll of all individuals who had entered the evacuated area should be taken to ensure that all have evacuated safely. If an evacuation or other emergency alarm sounds, guards and watchmen should take position at prearranged surveillance points to ensure that:

(1) Proper evacuation routes are being observed.

(2) SNM is not being tossed over the protected area perimeter barrier, and

(3) No one attempts to gain unauthorized access to the protected area during the emergency.

b. Failed Detection Equipment

Failed detection equipment should be repaired as quickly as possible. In the interim, alternate access or exit points or hand-held detection devices or hands-on search procedures should be employed. In no case should the failure of equipment be allowed to compromise the protection of the facility or the SNM within the facility.

PROTECTED AREA

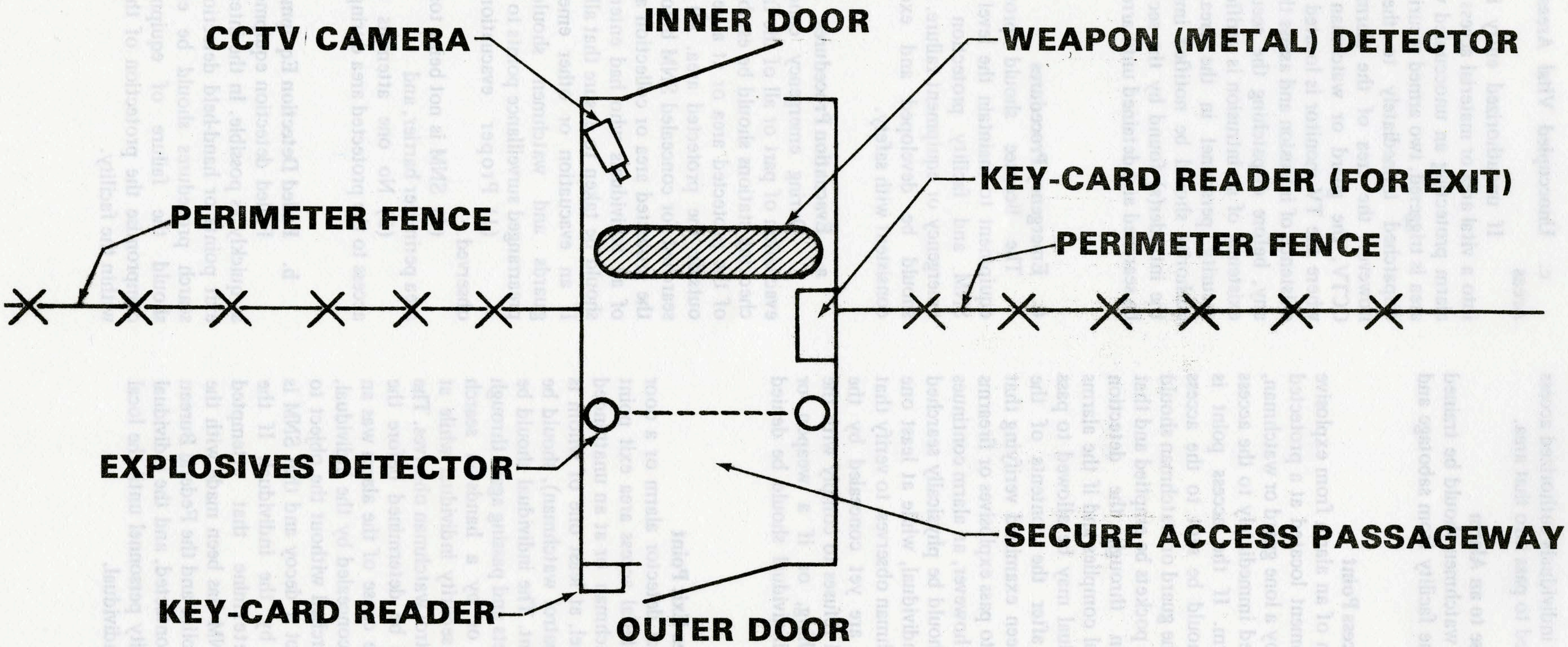
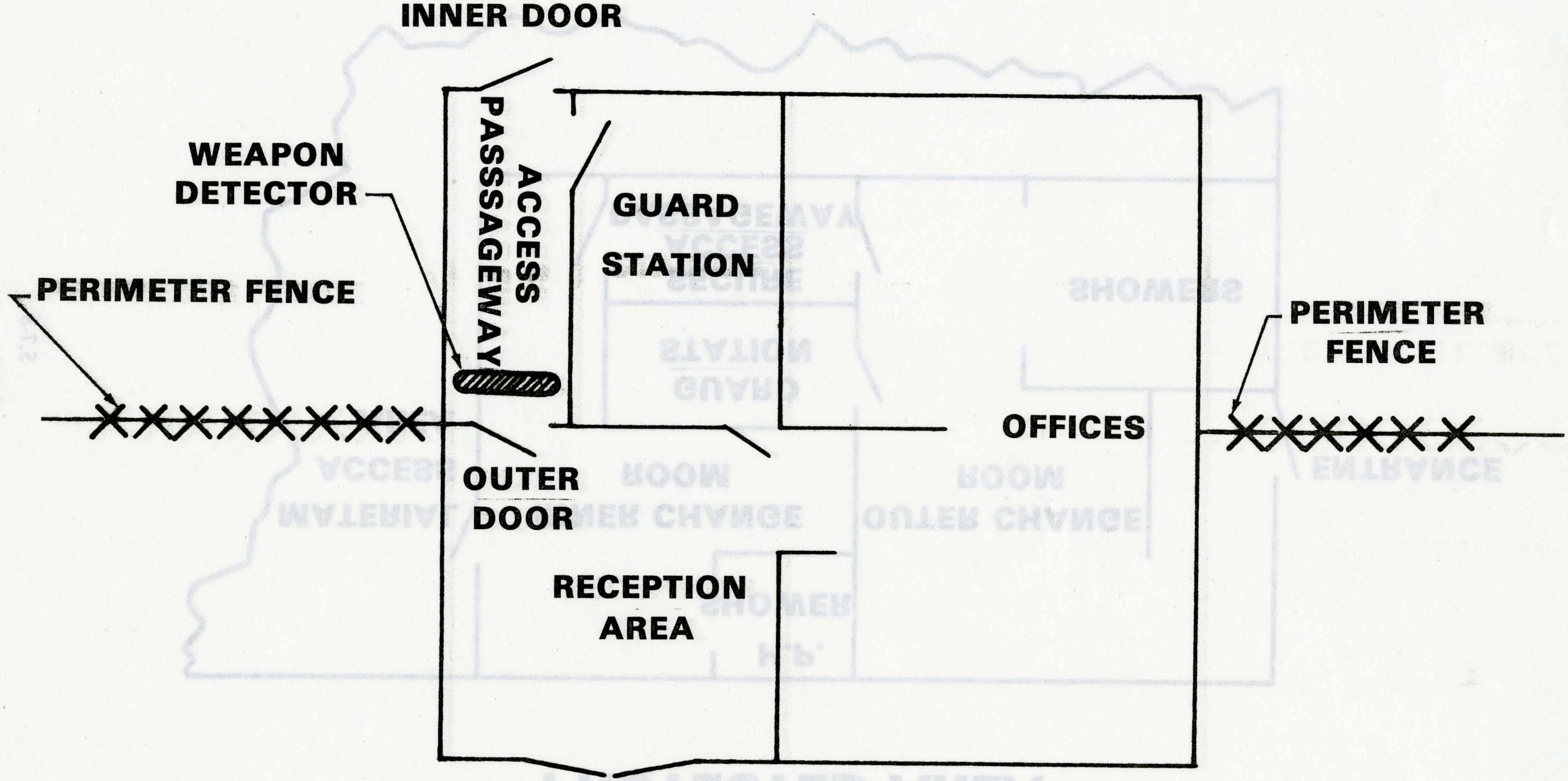


Figure 1

SECURE ACCESS PASSAGEWAY INTO PROTECTED AREA (UNATTENDED)

PROTECTED AREA

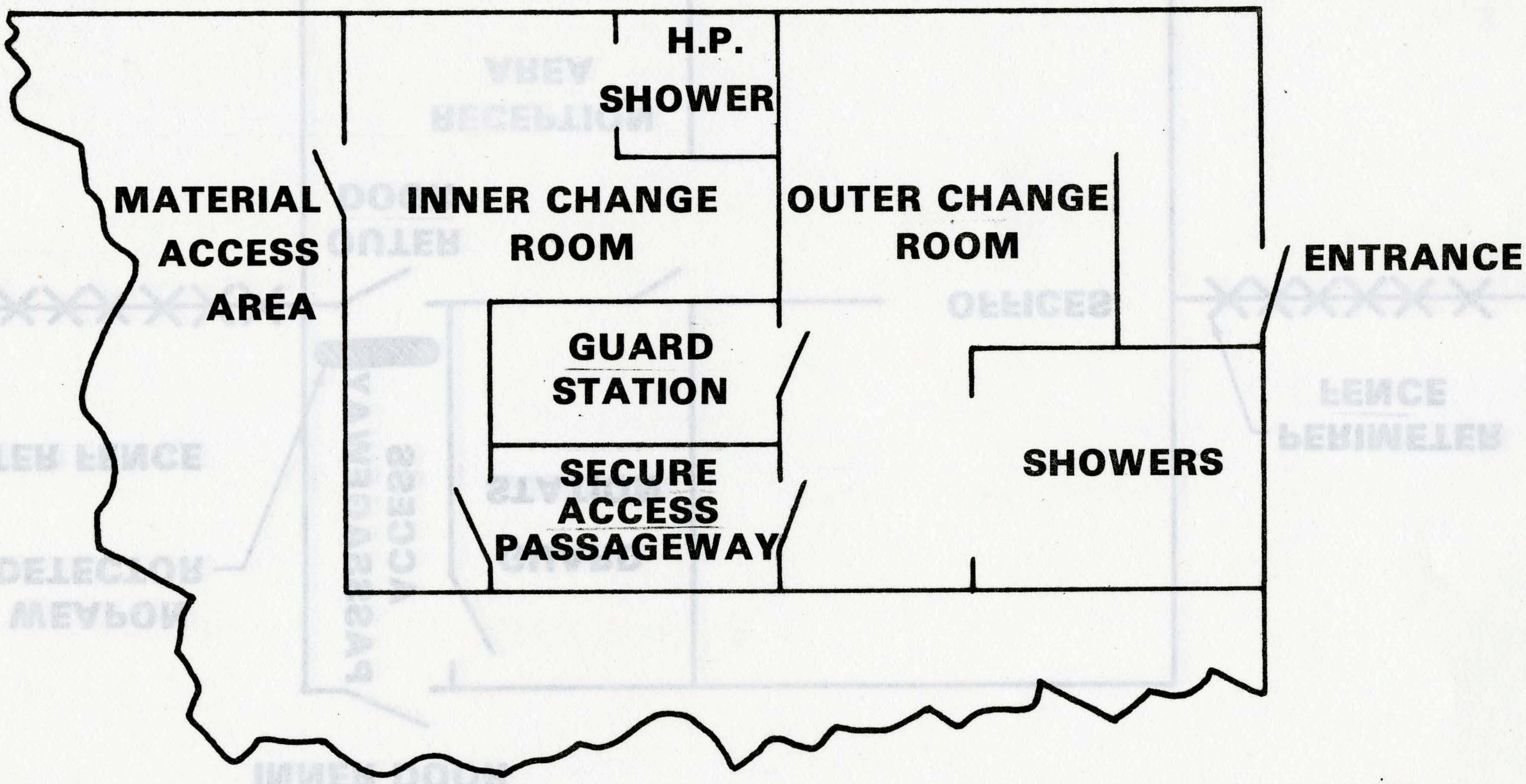


5.7-7

Figure 2

SECURE ACCESS PASSAGEWAY AT ENTRANCE TO PROTECTED AREA (ATTENDED)

PROTECTED AREA



5.7-8

Figure 3

SECURE ACCESS PASSAGEWAY BETWEEN CHANGE ROOMS

PROTECTED AREA

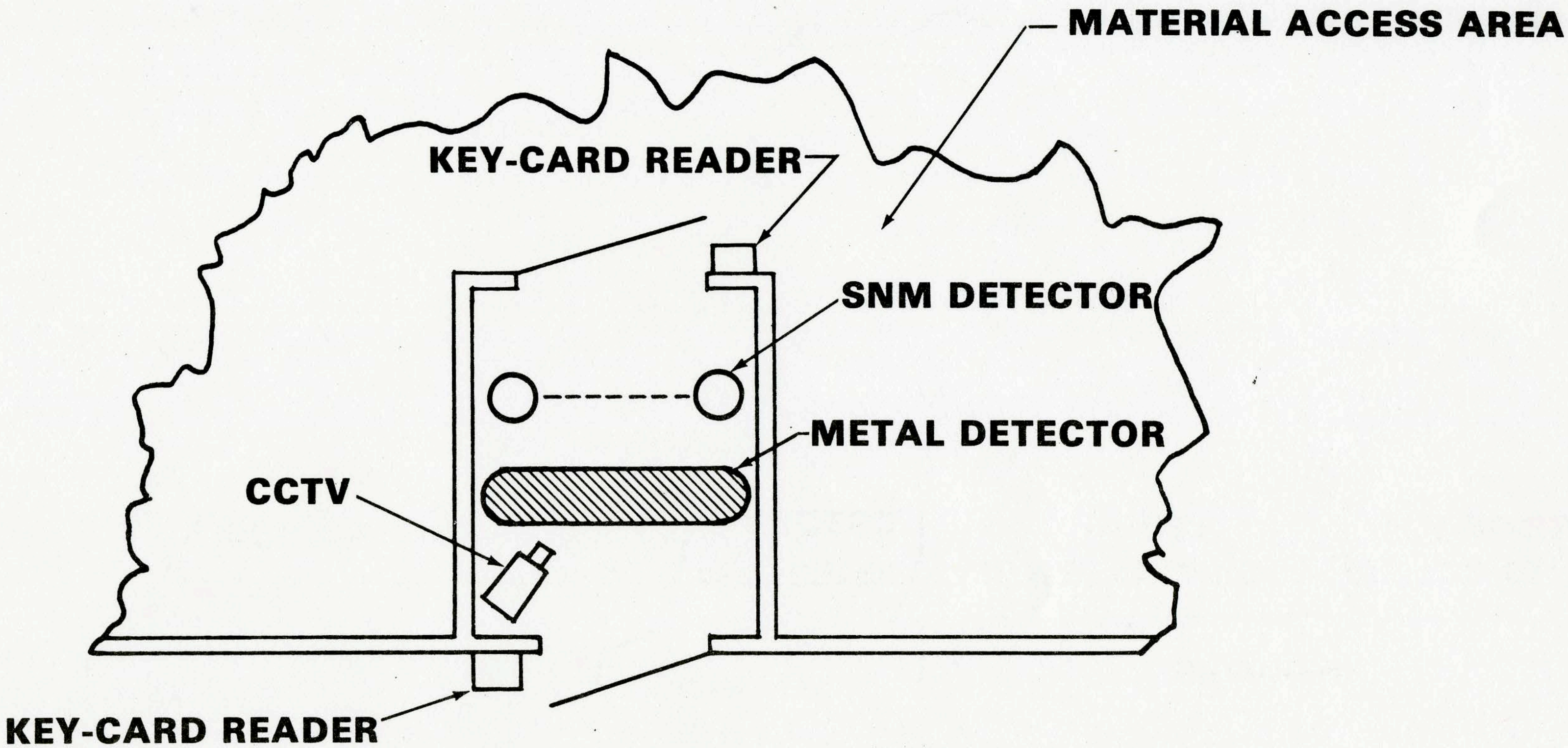


Figure 4
SECURE ACCESS PASSAGEWAY AT EXIT FROM MATERIAL ACCESS AREA

U.S. ATOMIC ENERGY COMMISSION
REGULATORY GUIDE
DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.10

SELECTION AND USE OF PRESSURE-SENSITIVE SEALS ON CONTAINERS FOR ONSITE STORAGE OF SPECIAL NUCLEAR MATERIAL

A. INTRODUCTION

Paragraph 70.22(b) of 10 CFR Part 70, "Special Nuclear Materials," requires that certain applicants for licenses to possess special nuclear material (SNM) provide a full description of their procedures for control of and accounting for the SNM possessed under license, including procedures used in storing said material. Paragraph 70.32(c) requires that licenses authorizing possession of certain quantities of SNM contain and be subject to a condition requiring the licensee to maintain fundamental material controls identified in Part 70 and other material control procedures deemed essential by the Commission for the safeguarding of SNM. Section 70.56 requires licensees to perform, or permit the Commission to perform, tests appropriate or necessary for the administration of the regulations in 10 CFR Part 70, including tests of equipment and devices used in connection with the production, utilization, or storage of SNM.

Pressure-sensitive seals on containers used for onsite storage of SNM are passive devices that indicate, upon inspection, whether tampering or entry has occurred. These seals may also serve as labels. This guide provides criteria acceptable to the Regulatory staff for selecting, affixing, and testing pressure-sensitive seals used for tamper-safing in connection with the onsite storage of SNM for compliance with the Commission's regulations with respect to material control.

B. DISCUSSION

The effective use of pressure-sensitive seals for tamper-safing containers of SNM in onsite storage should consider such basic elements as (1) composition, (2) seal properties, (3) method of affixing, (4) seal control, and (5) quality assurance.

1. Composition. The seal is basically a backing on one surface of which is a layer of adhesive covered by a protective liner.

The backing of pressure-sensitive labels or seals is usually made of paper, vinyl film, or plastic-coated paper and may be composed of more than one layer. To provide a consistent degree of adhesion, the adhesive on the backing should be aggressively tacky at room temperature and not require activation by water, solvents, or heat to form a bond to the container to which it is to be applied. Curing adhesives which harden as a result of exposure to air are not recommended because the initial adhesion should be adequate, and further adhesion only increases the difficulty of cleaning old seals from reusable containers.

The surface of the seal should carry a logotype to identify the licensee, and the complete surface of the seal should be covered with a regular and fine design to reveal erasures.

All seals should provide enough space to write by hand the type of material; the composition, weight, and serial number of items; the initials or signature of the person responsible for the statement of content; and the date of application of the seal.

Lettering on the seal, other than the logotype, should be large enough to be easily readable. The writing materials used to record information on the seals should be specified on the basis of qualification tests that establish compatibility with the surface of each type of seal.

2. Seal Properties. From the point of view of tamper resistance, the backing, adhesive, and ink of the seal should resist without damage all chemicals normally

USAEC REGULATORY GUIDES

present in the environment where the seal is to be used. For example, paper-base seals in general are sensitive to weather exposure; consequently, seals for exterior use should be made with a plastic base.

Any chemical capable of destroying or softening the adhesive should also destroy either the backing or the ink of the printing. This is particularly true of paper seals with acrylic adhesives that are most likely to tear when mechanical removal is attempted but are very permeable to solvents that attack the adhesive. Since the paper backing is usually not affected by the solvent, the ink used in the printing must be sensitive to such solvents in order to provide indication of tampering.

In general, paper backing on seals provides a surface capable of accepting various inks well because of the ease of wetting of the paper. Conversely, plastic backings, which are useful in applications requiring exposure to weather, tend to repel inks and have poor penetration, thus requiring special inks with surface active agents that ensure proper wetting of most plastics.

The seal backing should have a tear strength sufficiently low to provide an indication of tampering by careful peeling of the seal. The tear strength of the backing can be reduced and the peel force of the adhesive increased to the point where the peel test is satisfied. Another method of preventing peeling without tearing is to provide cross-shaped cuts in the backing.

Seals should be capable of withstanding normal or reasonably abnormal wear in use, without damage that would render the writing illegible or impair the detection of tampering.

3. **Method of Affixing.** It is important to affix seals properly in order to assure that SNM cannot be removed from a container without destroying either the seal or the container. Surfaces to which seals are to be applied should be clean and smooth. It is recommended that, for sealing cans, the seals be designed so they can be applied completely across the lid, extending at each end beyond the lid onto the body of the container for more than an inch. One such seal might consist of a T-shaped backing; the cross of the tee is the label with boxes for the handwritten information, and the upright of the tee is a tape long enough to extend completely across the lid.

4. **Seal Control.** Without adequate control of seals, replacement and subsequent duplication of the affixed seal would be more readily possible. There are two simple methods of preventing this type of replacement: strict control of the seal blanks and sequential numbering of the seals. As strict control of the seal blanks is difficult to maintain and verify, sequential numbering is preferred. However, for sequential numbering of seals to be effective, the seal numbers should be included in the record system, and the length of the number sequence should be adequate to prevent duplication of numbers in use at the facility. Only designated custodians or their alternates should have access to the seals or affix them to containers. The properties of the inks to be used for printing and recording have in common a sensitivity to the solvents that attack the adhesive. Thus seal numbers printed with such inks could be lost if accidentally damaged by solvents. To prevent this loss of identification of the container, the numbers should be printed with solvent-resistant inks or as perforations through the backing.

5. **Quality Assurance.** The licensee is responsible for demonstrating that the seals have and maintain the required resistance to and indication of tampering. Such a demonstration should include:

a. A solvent test in which an affixed seal sample is tested with a solvent to determine the effect on the adhesive, backing, and inks.

b. A peel test in which a tensile tester is used to determine the acceptability of the tear strength.

c. An erasing test in which rubber erasers and solvents are used to determine if any writing or printing can be erased without a clear indication of erasure.

C. REGULATORY POSITION

An acceptable program using pressure-sensitive seals to assist in assuring that the diversion or theft of SNM from containers in temporary onsite storage has not occurred and also to assist in assuring the validity of previously made measurements should give particular consideration to the composition, seal properties, method of affixing, seal control, and quality assurance.

1. **Composition.** The composition of a pressure-sensitive seal should include:

a. A backing or body usually made of paper, vinyl film, or plastic-coated paper;

b. An adhesive that covers one of the surfaces of the backing and is aggressively tacky at room temperature;

c. A liner that protects the adhesive and that is removed prior to affixing;

d. Logotype printing on the surface of the seal identifying the licensee;

e. A background printing of a fine design covering the complete surface of the seal;

f. Readable lettering.

2. **Seal Properties.** The properties of the seal components should be selected so that any attempt to tamper with the seal will be clearly indicated. The following requirements should be included:

a. The components of the seal should resist without damage all chemicals in the normal environment where the seal is to be used.

b. Either the backing material or printing inks should yield to chemicals that are capable of compromising the adhesive.

c. The tensile strength of the seal should be sufficiently low that any tampering by peeling will be indicated by tearing or delamination before the joint between the lid and the container is reached.

3. **Method of Affixing.** The method of affixing seals should include the following requirements:

a. The surfaces to which seals are to be applied should be clean and smooth.

b. A single continous seal, properly shaped, should be applied across opposite parts of the joint between the lid and the container, and the backing and adhesive should extend at least one inch on each side of the joint over a width of at least one-half inch. The seal should be affixed with sufficient tension to preclude the tilting of the lid allowing access to the contents without damage to the seal.

c. The seals should be applied immediately after the samples and data to identify and measure the contents have been taken.

4. **Seal Control.** In order to detect replacement or duplication of applied seals, strict control should be maintained over the seals in stock. Seal control should include the following requirements:

a. Seals should be available to and affixed and removed by only designated individuals responsible to material control and accounting management.

b. Seals should be sequentially numbered with sufficient alphameric or numeric digits to prevent duplication of numbers in use at that facility.

c. Sequential numbers on seals should be printed with solvent-resistant inks or as perforations through the backing.

d. Precise records of all the seals by number should be kept and should include pertinent data on the seal and data on the contents of the container. Such records should include any discrepancy that is observed in the container content, dates and times of application and removal of the seal, and the signatures of the individuals responsible to material control and accounting management for the data and for affixing and removing the seal.

e. Assurance should be required of the manufacturer that their masters of prenumbered seals and the scrap from fabrication are controlled.

5. **Quality Assurance.** The licensee should establish a quality assurance program to ensure that the seals conform to the above requirements. The quality assurance program should include qualification tests of seals at each time a new supply of seals is obtained and with existing stocks at intervals no greater than one year. The qualification tests should include a solvent test, a peeling test, and an erasing test. Tests requiring metallic surfaces should use stainless steel test panels; those requiring nonmetallic surfaces should use test panels of the same material as the container on which the seal is to be used. Acceptable test methods are described below:

a. **Solvent Test.** Samples should be prepared by affixing at least one square inch of seal material to a clean test panel of the proper material and rolling the sample with a 4-1/2-lb rubber-covered roller (ASTM Standard D2860-70, "Adhesion of Pressure-Sensitive Tape to Fiberboard at 90-Deg Angle and Constant Stress"[1]). Markings should be made on the seal materials with acceptable marking materials. At least five samples of seal material chosen at random from normally available stock should be tested with each solvent in the solvent test. The test panel and the samples adhering thereto should be immersed in the reagents identified and described in ASTM Standard D543-67, "Resistance of Plastics to Chemical Reagents,"[1 2] within 5 minutes of application and remain at room temperature for one-half hour.

If for any one sample, the seal material can be slid off the test panel, or if it falls free during or at the end of the period of immersion in any solvent, and if the backing and printing on a sample so removed remain unchanged, the sample and stock should be considered to have failed the test.

b. **Peel Test.** At least five samples of the seal material should be prepared and mounted on a test panel in the same manner as in Pressure Sensitive Tape Council Standard PSTC-5, "Quick Stick,"[3] except that the seal material in this test should be rolled with a 4-1/2-lb rubber-covered roller, as identified in C.5.a above, after application. The test panel should be mounted in a jig which is mounted on a tensile tester as per PSTC-5 and the tester started immediately at 0.2 inch per minute. This peel test should be conducted at a temperature of 23 ± 2 degrees Centigrade. If for any sample, as much as one-half inch of seal material can be peeled free without tearing or delamination, the sample and stock should be considered to have failed the test.

c. **Erasing Test.** Where the seal number is not perforated in the backing, at least five samples of the seal material containing the printed seal number should be affixed to a test panel. Rubber erasers and swabs moistened with all of the standard reagents as indicated in the solvent test should be used in attempts to erase the seal number. Each attempt should be limited to five minutes duration. If in any attempt, the printing can be erased without leaving a clearly apparent indication of erasure, the sample and stock should be considered to have failed the test.

---

[1] Copies may be obtained from American Society for Testing and Materials, 1916 Race Street, Philadelphia, Pennsylvania 19103.

[2] The specific standard reagents for the solvent test are in paragraphs 4.4.3, 4.4.7, 4.4.8, 4.4.12, 4.4.13, 4.4.15, 4.4.16, 4.4.19, 4.4.21, 4.4.28, 4.4.29, 4.4.31, 4.4.42, 4.4.45, 4.4.48, and 4.4.50 of ASTM Standard D543-67.

[3] Copies may be obtained from Pressure Sensitive Tape Council, 1201 Waukegan Road, Glenview, Illinois 60025.

November 1973

U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.12

GENERAL USE OF LOCKS IN THE PROTECTION AND CONTROL OF FACILITIES AND SPECIAL NUCLEAR MATERIALS

A. INTRODUCTION

Paragraph 50.34(c) of 10 CFR Part 50, "Licensing of Production and Utilization Facilities," requires each application for a license to operate a production or utilization facility and paragraph 70.22(b) of 10 CFR Part 70, "Special Nuclear Material," requires certain applications for a license to possess or use special nuclear material (SNM) to include a physical security plan to demonstrate how the applicant plans to meet the physical protection requirements of 10 CFR Part 73, "Physical Protection of Plants and Materials." Paragraphs 50.54(p) and 70.32(e) require existing licensees licensed under Part 50 and certain licensees licensed under Part 70 who have not submitted a physical security plan to submit such a plan to the Commission for approval. Section 73.40 of 10 CFR Part 73 requires that certain licensees provide physical protection against industrial sabotage and against theft of SNM at the fixed sites where licensed activities are conducted.

Locks are acceptable devices to be used in adhering to the physical protection requirements identified above to assist in controlling access to areas, facilities, and materials through doors, gates, container lids, and similar material or personnel access points, and are considered essential components of a physical barrier. This guide provides criteria acceptable to the Regulatory Staff for the selection and use of commercially available locks in the protection of facilities and SNM.

B. DISCUSSION

Locks are very important components of a physical barrier. Their effectiveness, however, lies in their use in conjunction with other security measures such as intrusion alarm systems and seals. Although some locks are difficult to pick or manipulate, no lock can claim to be "manipulation proof." Because of the large variety of locks available, it is necessary to subdivide the discussion on locks into the following types: (1) combination, (2) key, (3) electrical, and (4) pushbutton mechanical locks. The discussion of each type includes a general section on advantages and disadvantages, a section on control over the locks, and a section on the applicable standards and specifications.

1. Combination Locks

a. **General.** It is desirable that a combination lock be designed to afford a choice of a large number of combinations. The number of combinations is determined by the number of tumbler wheels in the lock mechanism and the number of graduations on the dial. High-quality locks usually have 100 divisions on the dial and three tumbler wheels; such a lock is capable of providing a theoretical 10^6 combinations which in practice reduces to tens of thousands. Some combination locks are made with four tumbler wheels, but it is considered that the added number of combinations possible does not proportionally improve the security of the lock and does increase the inconvenience of dialing the combination.

It is desirable for a combination lock to be designed so its combination can be easily changed but at the same time be tamper resistant. The combination of some locks can be changed by disassembly of the tumbler wheel pack and relocation of screws or pins. In this method the effective number of combinations possible is restricted. Another method involves taking apart the wheel pack and resetting an insert in each wheel. This method requires substantial skill on the part of the operator. The most desirable method of changing a combination is by a special key which requires minimal training of the operator and provides a maximum number of combinations. The special key is inserted in

USAEC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the AEC Regulatory staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Published guides will be revised periodically, as appropriate, to accommodate comments and to reflect new information or experience.

Copies of published guides may be obtained by request indicating the divisions desired to the U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Director of Regulatory Standards. Comments and suggestions for improvements in these guides are encouraged and should be sent to the Secretary of the Commission, U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Chief, Public Proceedings Staff.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust Review
10. General

the back of the lock case to release the wheels from their present combination while a new combination is imposed by dialing.

The combination of some locks can be covertly determined by using a radiographic technique. Resistance to this form of attack is designed into certain locks by utilizing materials in the mechanism that are not easily radiographed, e.g., plastics.

Combination locks are vulnerable to compromise if the back of the lock is readily available, e.g., when the lockable access is open. Removing the back cover from the lock usually allows the combination to be determined. The combinations of some key-change locks can be changed directly when the lock is in the open position, while other must have the existing combination redialed to a different index when the access is in the open position to permit the combination change. The former type permits an intruder to make a quick change of the combination to one of his own choosing; this would permit him to enter following the closing of the lock and would deny entry to the user. For these reasons it is desirable to protect the back of the lock by back plates or other devices.

High-quality combination locks are designed for use in two basic forms: (1) in a lock case to be mounted on or into a door as a mortise or rim lock and (2) as a padlock.

Protection against forcible attack of a mortise or rim-mounted lock can be increased if the lock is provided with hardened steel plates and if the lock is designed with relocking triggers or devices that deadlock the bolt or bolt-actuating mechanism.

Combination padlocks are not vulnerable to the usual rapping techniques and are usually resistant to manipulation. However, common combination padlocks made of a cast aluminum alloy are without great strength, have little resistance to forcible attack, and are not weather resistant. There are others that are weather resistant but offer little protection against attack.

b. **Combination Lock Control.** The most important aspect of lock control for combination locks is the protection of the combination. It is desirable to change the combination of a lock every time that a person who knows the combination no longer requires it as a result of termination or reassignment of duties. This would assure that only those individuals actually required to gain access would know the combination.

Losing the combination of a manipulation-proof, well-designed lock in a high-rated door is an expensive situation. This can be prevented by keeping a record of the combination in another location which is as secure as the place protected by the lock.

Combination locks can be set to a single number to simplify the daily chore of opening, but this is a very poor practice since it reduces the security of the lock. Frequently four-wheel locks are set to only three different numbers for ease of opening. This defeats the purpose of the fourth wheel but it is not considered serious since the number of remaining combination choices is considered adequate. It is not recommended that one select combinations in common sequences and multiples of ten. It is also not generally recommended that the last number of a combination be set close to zero because in some cases the lock can jam.

c. **Standards and Specifications.** A standard for three- or four-tumbler combination locks issued by Underwriters' Laboratories, UL-768, "Combination Locks,"[1] covers "combination locks designed for attachment on doors of safes, chests, vaults, and the like to provide a means of locking the boltwork against unauthorized opening." Quality assurance provisions covering the description, examination, and testing of the product are included through the UL Label Service. A Federal Specification issued for combination padlocks, FF-P-110F, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack),"[2] includes quality assurance provisions for design, materials, and performance testing.

2. Key Locks

a. **General.** As in the case of combination locks, it is desirable for a key lock to be capable of being set for a large number of different keys. A high-quality six-pin lock with 10 key cutting levels per pin potentially permits 10^6 different keys to be used. However, this large number of key cuts is not as useful as a large number of combinations because less time-consuming techniques for defeating key locks are available. Nevertheless, there is value in specifying at least 10^6 key cuts because it requires careful construction of the lock.

It is important that the key cut required to open a lock (bitting of a lock) be changeable to permit changes whenever keys are lost or an employee having access to a key is reassigned to other duties or

---

[1] Copies may be obtained from the offices and testing stations of Underwriters' Laboratories, Inc. located at the following addresses: 207 East Ohio Street, Chicago, Ill. 60611; 333 Pfingsten Road, Northbrook, Ill. 60062; 1285 Walt Whitman Road, Melville, L.I., N.Y. 11746; 1655 Scott Boulevard, Santa Clara, Calif. 95050.

[2] Copies may be obtained from business service centers of the General Services Administration Regional Offices located in the following cities: Boston, Mass.; New York, N.Y.; Washington, D.C.; Ft. Worth, Texas; Denver, Colo.; San Francisco, Calif.; Atlanta, Ga.; Chicago, Ill.; Kansas City, Mo.; Los Angeles, Calif.; Seattle, Wash.

terminated. Changing the bitting of a lock can be accomplished usually by changing pins, wafers, or levers. To ease the task of a bitting change, some locks have cores that are removable for replacement by means of a special key called a "control key." If all the locks in a given facility are keyed to the same control key, the locks are virtually master keyed because, with the core removed, the problem of opening the lock is elementary.

Master keying is undesirable from a security point of view because disassembly and inspection of any lock in the system by a competent person provides access to all the other locks in the master-keyed system, and because termination of an employee who had access to a master key would require changing the bitting of all locks set for his master key. The changing of the bitting of a large number of locks can be costly, but the convenience of master systems is such that there is strong pressure for using them. A compromise in this conflict between convenience and security may be to use a nonmastered set of locks for protected areas, material access areas, vital areas, and access to vital equipment and to permit master key sets for other less sensitive areas.

It is necessary for a lock to have some resistance to picking and impressioning (a method used to prepare a key by the impressions of the bitting of a lock on a blank key). In general, this resistance can be provided by precision machining of the mechanisms or by special design features such as side bars, odd-shaped pins or a large number of levers.

Protection of key locks against forcible attack can be enhanced by the use of hardened steel plates in front of the pins or side bars.

It is essential for a bolt of a lock to be retained in the locked position by positive means (dead bolt). In some locks, the bolt is held in a locked position by a spring only. This permits, in the case of padlocks, the use of appropriate rapping or shimming techniques and, in the case of door locks, the opportunity to surreptitiously retract the bolt without the use of force.

b. Lock Control. The security of an access control system based on key locks depends on complete denial of keys to unauthorized persons. It is essential to have a record of each key and the names of individuals to whom keys have been issued and to check all keys at periodic intervals.

A common weakness in mastered key systems is the lack of accountability of lock cylinders. To correct this situation, it would be necessary to require a control system involving the accountability of every mastered lock cylinder having the bitting in present use either for the master or, in the case of removable cores, the control key.

c. Standards and Specifications. A standard for key locks has been issued by Underwriters' Laboratories, UL-437, "Key Locks,"[1] and includes quality assurance provisions through the UL Label Service. Interim Federal Specification FF-P-001480 (GSA-FSS), "Padlock, Key Operated (Resistant to Opening by Force, Pick, and Bypass Techniques),"[2] covers two types of key-operated dead-bolt padlocks: the exposed shackle and the shrouded shackle. Quality assurance provisions concerning the design, materials, and qualification testing are included.

3. Electric Locks

a. General. In the most popular electric locks, a signal generated by magnetized elements in a plastic card or by sequential activation of buttons is compared with a stored code to activate an electrically operated door strike. In some cases the magnetic card and pushbutton systems are used in coincidence. Combined card and pushbutton systems provide, in general, higher security than card-only systems.

The advantages of the electric lock are isolation of the part containing the code from the exposed part of the lock, versatility of programming, and ease of integration into alarm systems.

Magnetic card systems have some of the problems of common key locks because a lost or stolen card can be used by an unauthorized person. However, reproduction of a card is more complicated than reproduction of a metal key.

Pushbutton systems require memorization of a few digits, usually four, and require more time to operate than the magnetic card system. Although the number of possible combinations usually is smaller than in the combination lock system, quality electric pushbutton systems compensate for this by incorporating devices which prevent trial and error methods of surreptitious attack by activating an alarm after a number of unsuccessful attempts or by introducing a delay after each unsuccessful attempt which prevents operation of the lock for a short period of time.

It is desirable for an electric lock to have the capability for an easy change of combinations. The part of the lock where the combination is set and the housing of the card reader (if the contents of the housing can reveal the combination) should be protected against tampering by tamper switches connected to the alarm system.

Generally, where electric locks are installed, a mechanical lock is also installed as a bypass. This lock should be of a quality as discussed in the part on key locks in this guide.

b. **Lock Control.** The security of an electric lock system depends on strict control of combinations and cards. The magnetic codes in the cards and the combinations need to be changed whenever an employee having had access to them terminates or is reassigned. Strict accountability of cards is strongly recommended.

c. **Standards and Specifications.** There are currently no comprehensive standards or specifications covering electric locks. The reputation of the manufacturer, the specification for his product, and the experience of users must be carefully considered in their selection and use.

4. Pushbutton Mechanical Locks

a. **General.** This is a type of combination lock utilizing mechanical-pushbutton-activated linkages that connect a gate with an external knob to permit opening of the lock. In this lock it is difficult to design in penalties for punching a wrong combination as is done in electric locks. Therefore, it is important to have a large number of possible combinations.

Provisions for easy change of combinations are desirable. Some locks permit a new combination to be dialed in utilizing an Allen wrench when the lock is open, a procedure similar to that for some combination locks. Others require the replacement of internal parts to change the combination.

The mechanical locks appear to be fairly resistant to concealed attack; however, more information is needed on their resistance to forcible attack.

b. **Lock Control.** Similar to other combination locks, the combinations need to be changed when employees having access to the combination terminate or are reassigned.

c. **Quality Assurance.** There are currently no comprehensive standards or specifications for mechanical pushbutton locks.

C. REGULATORY POSITION

The following guidelines are acceptable to the Regulatory staff for the selection and use of locks in the protection of facilities and SNM:

1. **Combination locks** installed in solid doors such as those in vaults or vault-type rooms in protected areas should be three- or four-position dial-type changeable-combination locks meeting the Underwriters' Laboratories Standard UL-768, "Combination Locks," for Group I locks.[1]

2. **Combination padlocks** should be used when practicable on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment in preference to key padlocks. Combination padlocks should be used on closed vehicles or containers holding SNM that are required to be locked. Combination padlocks should be three-position-dial type changeable-combination padlocks meeting Federal Specification FF-P-110F, "Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack)."[2]

3. **Key locks** used in lieu of combination padlocks on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment should provide a high degree of resistance to opening by force and tamper techniques and should meet Underwriters' Laboratories UL-437, "Key Locks."[1]

4. **Key padlocks** used in lieu of combination padlocks on doors or gates to material access areas, in protected and vital area perimeters, and for access to vital equipment should be of rugged and sturdy construction and designed for outdoor use if necessary, and should meet Interim Federal Specification FF-P-001480 (GSA FSS), "Padlock, Key Operated (Resistant to Opening by Force, Pick, and Bypass Techniques)."[2]

5. **Electric locks** should be used inside the protected area as a means of access control only if a magnetic card key system is coupled with a pushbutton system and integrated into the alarm system. This lock combination should have features that resist tampering with the combination-changing mechanism and that alarm after a set number of errors in punching the combinations is made.

6. **Pushbutton mechanical locks** are not recommended for use at this time because of the lack of comprehensive standards and specifications against which the locks can be evaluated.

7. **Mechanical locks** used as panic locks on emergency exit doors within protected area perimeters should be operable only from the inside.

8. **Combinations, keys and locks** should be controlled, protected and changed in accordance with the following requirements:

a. Combinations of locks or padlocks on repositories containing SNM or used to secure gates or doors to material access areas, in protected and vital area perimeters, and for access to vital equipment should be known only to those authorized access to the material or to the area. They should be changed when repositories or areas are first placed in use, whenever a person knowing the combination no longer requires it as a result of reassignment of duties or termination, whenever the combination may have been compromised, or at least twice every year. A record of the combinations of locks should be kept in a location that is secured by a combination lock.

b. Keys and cards to locks or padlocks on containers holding SNM or used to secure gates or doors to material access areas and in protected and vital area perimeters should be issued only to persons authorized access to the material or to the area. Keys or cards in use should be checked in at the end of each shift or workday, and a log should be maintained showing keys and cards, users, in and out times, and other pertinent information. Keys and cards should be recovered from reassigned or terminating personnel. Locks should be immediately changed or cores replaced and an inventory conducted whenever a core, key, or card is lost or missing; the lock, core, key, or card has been compromised; or unrecorded keys or cards are found. In a mastered system, a complete remastering of the system should be conducted whenever a core, card, master or control key, or a lock is lost or compromised.

c. A record of all locks, cores, keys, and cards should be maintained and kept in a location secured by a combination lock. A physical inventory of locks, cores, keys, and cards should be conducted semiannually when the locks are used for protection of facilities and bimonthly when the locks are used for the protection of SNM. Unused locks, cores, keys, and cards should be stored in a location secured by a combination lock. A specific individual at each site should be named and placed in charge of all locks, cores, keys, and cards.

U.S. ATOMIC ENERGY COMMISSION

November 1973

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.14

VISUAL SURVEILLANCE OF INDIVIDUALS IN MATERIAL ACCESS AREAS

A. INTRODUCTION

Title 10 CFR, Part 73, "Physical Protection of Plants and Materials," delineates requirements for the physical protection of licensee plants and the special nuclear materials used, stored, or processed therein. Paragraph (a)(7) of § 73.60,[1] "Physical Protection of Special Nuclear Material at Fixed Sites," specifically requires that the licensee provide and use on a continuing basis methods to observe individuals within the material access areas to assure that special nuclear material is not diverted. Visual surveillance techniques (e.g., closed-circuit television, observation galleries, or direct visual observation by fellow workers or special surveillants), if used to meet this requirement, can be aided by proper consideration of surveillance requirements both in the initial phases of plant construction and the installation of process equipment and in the continuing development of operating procedures and administrative controls.

This guide describes operational measures and physical features which the AEC Regulatory staff considers to be adequate for the implementation of visual surveillance. Such measures are generally not dependent on the nature of the process operations planned for a particular plant. However, specific physical features (for example, glove box enclosures) may not be applicable to all plants.

B. DISCUSSION

1. Objective of Surveillance

Effective surveillance of individuals having access to special nuclear material (SNM) can enhance the protection and/or probability of recovery of such material in the following manner:

a. The likelihood of diversion will be reduced. An individual who is aware that his actions are being monitored will tend to be deterred from illegal acts.

b. Diversion can be detected. Information can be obtained about the identities and activities of individuals suspected of diverting or attempting to divert SNM from a specific unit process or location in the material access area.

c. The capability of recovering diverted material is enhanced. When material is discovered to be missing, reconstruction of the diversion event may be possible from routine surveillance information.

d. Surveillance can provide a backup to access control. The presence of unauthorized individuals in a material access area or the nonessential presence of personnel normally authorized access can be observed and documented.

2. Scope of Surveillance

As used herein, visual surveillance means the direct or indirect observation of individuals to detect activities potentially involving access to special nuclear material for diversion.

In some special cases, visual surveillance (observation) may be replaced by deductive surveillance to assure that special nuclear material is not diverted. For example, if the only special nuclear material allowed in a particular material access area is of a size, weight, or form such that unauthorized removal would be readily detected *and* this material cannot be clandestinely subdivided into concealable size, weight, or shape, then visual surveillance of individuals in that material access area may be unnecessary. Similarly, if the only SNM in an area is contained in instrumented packages (e.g., a specially designed vault or automated or remotely

[1] 38 F.R. 30537, 11/6/73.

controlled process equipment) so that any attempt to surreptitiously remove the SNM (such as by attempted bypassing of protective devices or use of manual override options) will be indicated at a manned control console *and* the individual manning the console will interpret the indication as a potential theft attempt *and* annunicator systems will assure his cognizance of such an indication, then visual surveillance may not be necessary.

Further, different visual surveillance methods may be appropriate to specific parts of a particular facility and for specific purposes. While direct observation may be required for high-risk areas, closed-circuit television may be suitable for others. Information obtained and analyzed immediately could be used to prevent a diversion while information suited to later analysis could be used to identify and apprehend the diverter who may have eluded initial detection.

3. Management Support

A well-designed or well-equipped surveillance system will not function satisfactorily without a company-backed policy for proper utilization of the system. Without proper attention to operating procedures, a diversion may be difficult to detect and diverted material much more difficult to recover.

If a surveillance system is to be effective, a sufficient number of surveillants must be available to observe processes and individuals during normal operation, during shift change, when the process is shut down such as at night or on weekends, and when conditions are not normal such as during a physical inventory or during an emergency.

4. Surveillance Personnel

Surveillance personnel may include guards, watchmen, management personnel, remotely located surveillants and/or fellow workers. To be effective, the surveillant must be familiar enough with the operation he is witnessing to be capable of detecting activities that are not authorized or are inconsistent with established materials protection procedures.

Surveillance, whether by fellow workers or others, is subject to certain inherent problems. The use of pairs of workers to observe each other is susceptible to collusion between the two. While this susceptibility can be reduced by rotating the activity assignments of individuals so as not to have set pairs, any surveillance system that relies heavily on fellow worker surveillance must recognize the inherent reluctance of most employees to report a fellow worker. On the other hand, a surveillance system that relies extensively on watchmen, uniformed guards, and remote viewing devices can adversely affect employee morale. A concerted effort by management to instill in its employees a sense of mutual responsibility for the protection of SNM (similar to current safety awareness campaigns which usually combine features of both "fellow worker" and "outsider" surveillance) can serve to counteract these disadvantages.

5. Surveillance Instrumentation

The surveillance function can be aided by either optical (mirrors, periscopes, etc.) or electronic (closed-circuit television) hardware systems. Closed-circuit television cameras offer greater operational freedom since they can be mounted on a remotely positioned base and can be equipped with remotely operated pan, tilt, and zoom controls. In either case, the system can be augmented by photography or video tape to provide permanent records for later use. The recording system can also be activated by a command signal from an intrusion alarm to automatically provide a record of any action or irregularity following the indication of intrusion.

6. Physical Characteristics

Any interference in the capability to monitor the activities of an individual presents a problem for effective surveillance. This interference may result from unnecessarily complex operating procedures or from inherent physical limitations such as inadequate visibility resulting from poor lighting or the presence of smoke, steam, or fumes or the presence of partitions, physical obstructions, or shielding. To reduce the effect of floor level obstructions, elevated viewing galleries have been used.

C. REGULATORY POSITION

In addition to the immediate area where SNM is processed or stored (which must be in a material access area[2]), all areas accessible from an SNM process or storage area without a check of individuals and packages for concealed SNM[3] are considered a part of a material access area and when occupied must be provided with a means of observing individuals therein. While visual surveillance techniques are generally applicable to all SNM processing or storage activities, proper attention to SNM storage restrictions (size, weight, form) and protective instrumentation can, in lieu of visual observation, deductively provide assurance that SNM cannot be diverted from or through the area. This section describes operational measures and physical features which will aid the use of visual surveillance for the protection of special nuclear material.

---

[2] §73.60 (a)(1) of 10 CFR Part 73.

[3] See Regulatory Guide 5.7, "Control of Personnel Access to Protected Areas, Vital Areas, and Material Access Areas.

1. **Operational Measures**

The following guidelines set forth features and characteristics of administrative and procedural measures acceptable to the Regulatory staff for assuring that satisfactory visual surveillance can be maintained.

a. **Administrative Controls**

(1) All facility personnel should be instructed in the objectives of the surveillance system and how it operates. Individuals whose primary responsibility is surveillance (e.g., escorts, watchmen, or guards should be trained [4] in the use of surveillance aids and should be sufficiently familiar with routine plant operations and special purpose activities to be able to recognize irregular procedures.

(2) A surveillance system relying on fellow worker surveillance must recognize the reluctance of most employees to inform authorities on the misdeeds of their companions. If utilized, special attention should be given to a program aimed at instilling in each employee a sense of personal jeopardy as a result of a theft of SNM by a fellow worker.

(3) Surveillance policies for emergency situations should provide for continued surveillance of personnel evacuating the material access area until they have been checked for concealed SNM, for remote surveillance of the evacuated area while not compromising the surveillance of other areas that may not have been evacuated, and for temporarily assigning special surveillance activities as may be required. (A more detailed description of emergency measures is to be included in another regulatory guide dealing with materials protection under emergency conditions.)

b. **Operating Procedures**

(1) The surveillance system should be tested periodically and the results of those tests documented.

(a) The range and clarity of fields of view, including the vulnerability of hardware components to interferences from fluorescent lighting or sources of vibration, heat, or electric fields, should be checked.

(b) The adherence to required reporting procedures [5] should be verified.

(2) Equipment, supplies, and byproducts that are used or are produced in the material access area should be kept in designated storage locations when not in use and should not be allowed to accumulate where they can interfere with surveillance.

(3) All aisles and passageways through a material access area should be kept free of temporarily stored process materials, scrap, and trash so as not to interfere with surveillance of the area.

2. **Aids to Effective Surveillance**

Whether direct or indirect visual observation techniques are used, the following physical features are acceptable to Regulatory staff to assure a capability for effective visual surveillance. Dimensional guidance is based on generally accepted industrial practice.

a. **Area Characteristics**

(1) An area where SNM is processed or stored should be provided with lighting capable of illuminating equipment and working surfaces with no less than 50 ft-candles during normal working hours or when otherwise occupied. [6,7]

(2) Support areas or other "nonprocess or nonstorage" locations within a material access area should be provided with lighting capable of illuminating the area with no less than 30 ft-candles during normal working hours or when otherwise occupied. [7]

(3) If obstructions (e.g., room partitions, screen panels, radiation shielding, and safety barricades) interfere with direct surveillance of process aisles, process equipment, or operators, special vantage points, mirrors, or remote viewing devices should be provided.

(4) Storage areas for in-process, feed, product, scrap, and waste materials containing SNM should have sufficient capacity that material can be stored in designated locations in a manner that will not interfere with lighting or the field of view of surveillance devices. If storage is above floor level, the area should be arranged with clearly defined aisles between storage racks and shelves. Each aisle that provides access to SNM should be capable of being monitored by direct or indirect visual surveillance. If storage is below floor level (e.g., in trenches or individual pits) the area should be free of partitions, obstructions, or structures above floor level that could conceal an individual from view.

(5) Containers of SNM in storage should be arranged so that covers and seals are visible from adjacent aisles or passageways and from a distance of at least 5 feet.

(6) Shipping and receiving areas should be arranged with sufficient clear space that movement of an individual around vehicles in the area can be observed. The dock area adjacent to the cargo portal of a vehicle being loaded or unloaded should be kept clear of objects which could obstruct observation of activities within 20 feet of the portal.

[4] A regulatory guide on the training, equipping, and qualifying of guards and watchman is under development.

[5] Includes reports to the AEC and the facility security organization as necessary pursuant to § § 73.71(b) and 73.50(g), respectively, of 10 CFR Part 73.

[6] Intrusion alarms are required for such areas when unoccupied pursuant to § 73.60(c) of 10 CFR Part 73.

[7] ANSI Standard A11.1-1973, "American National Standard Practice for Industrial Lighting." Copies may be obtained from the Illuminating Engineering Society, 345 East 47th Street, New York, New York 10017.

b. Process Equipment Characteristics

(1) Surveillance devices or stations should be located so that access ports (covered or in use) or bag out stations of enclosed process lines (glove boxes or hoods) will not be obscured from view.

(2) Where posible, material protection devices on, or associated with, process equipment and including auxiliary surveillance equipment itself should be equipped with alarms to signal the surveillant of tampering. Where closed-circuit television with video tape recording is used, it should be coupled to the intrusion alarm system so that an indication of an intrusion will automatically actuate recording equipment.

(3) Surveillance devices or stations should be located so that heating and ventilating ducts, utility piping, conduit, or other items providing services to process equipment or equipment enclosures do not block observation of work areas.

(4) Process equipment that normally contains SNM should be so arranged (or designed) that openings and drains used to remove liquids, slurries, and dry materials (including samples) from the equipment operate in either a fully open or fully closed mode which is determinable (verifiable) from a distance of at least 10 feet.

(5) The boundaries of areas dedicated to a particular process or, in the case of parallel process lines, to a particular line should be clearly marked (e.g., with colored floor tile, painted lines). Clearly marked aisles not less than 8 feet in width should be located between equipment or equipment enclosures that constitute separate process lines or functions.

(6) Piping, ducts, or conveyor systems used to move SNM within a process, from one process to another process, and to or from storage should be distinctly marked (e.g., color coded) to identify the contents.

(7) All containers for SNM should be designed so as to have characteristic markings and characteristic colors or shapes to identify whether the SNM is buffer storage, final product, scrap for recycle, scrap for recovery, or waste. These containers should also be distinguishable from all other containers in the area.

[8] See also other regulatory guides dealing with the design of process equipment (e.g., Regulatory Guide 5.6, "Design Considerations for Minimizing Residual Holdup of Special Nuclear Material in Drying and Fluidized Bed Operations").

January 1974

U.S. ATOMIC ENERGY COMMISSION
REGULATORY GUIDE
DIRECTORATE OF REGULATORY STANDARDS

REGULATORY 5.15

SECURITY SEALS FOR THE PROTECTION AND CONTROL OF SPECIAL NUCLEAR MATERIAL

A. INTRODUCTION

Paragraph 70.51(e) of 10 CFR Part 70, "Special Nuclear Material," requires that certain licensees authorized to possess at any one time special nuclear material (SNM) in a quantity exceeding one effective kilogram maintain, among other things, procedures for tamper-safing containers or vaults containing SNM not in process, control of access to devices and records of the date and time of application of each device to a container or vault, unique identification of each such item, and other pertinent records of all such items. Paragraph 73.30(c) of 10 CFR Part 73, "Physical Protection of Plants and Materials" requires, among other things, that SNM be shipped in containers which are sealed by tamper-indicating type seals and that, except under certain conditions, the outermost container or vehicle also be sealed by tamper-indicating type seals. Paragraph 73.41(c) requires, among other things, that each licensee keep records of shipments of SNM subject to the requirements of this part, including seal descriptions and identification and that such information be recorded prior to shipment. This guide identifies features of security seal systems and describes types of seals that are generally acceptable to the Regulatory staff for tamper-safing of SNM.

B. DISCUSSION

Security Seals

A security seal is a passive device used to detect tampering or entry. Various types have been developed to meet specific requirements. The different types of seals retain essentially the same elements but with varied emphasis.

A property common to all types of seals is frangibility. A seal is not expected to present a serious obstacle to entry or tampering, and for that reason it is usually a rather weak mechanical obstruction which can be overcome with small effort. Some seals, such as those utilizing sealing wax, are brittle. This property of seals is, in certain cases, intentionally enhanced, as in the case of prestressed glass containers used as seals to define a secure volume. Here, the stored energy serves to shatter the glass if excessive force is used. In some metallic seals, notches are cut so that if one attempts to bend back the essential part of the seal to reclose it, the metal breaks from fatigue along the notched part.

Seals are passive devices requiring inspection to indicate whether entry or tampering has occurred. An unalarmed glass door is a seal in the sense that it is frangible and passive. On the other hand, the wall of a vault is a passive barrier but is not frangible and is therefore not commonly considered to be a seal.

Seals are nonreversible in the sense that once broken, they are difficult to reassemble without leaving signs of the reclosing.

Seals are identifiable, in that it is possible to add unique identification characteristics, allowing detection of whether the seal is the one originally applied and not a forgery. This property, however, is sometimes replaced by limiting the availability either of the seals in the unapplied state or of some part of the sealing procedure. Resorting to limitations on availability to replace identification procedures is now recognized to be a poor practice. This is probably one of the most important evolutionary changes observed in seals. It appears that, in early sealing wax seals, the main emphasis was on protection of the tool used for impressing the hot sealing

USAEC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the AEC Regulatory staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Published guides will be revised periodically, as appropriate, to accommodate comments and to reflect new information or experience.

Copies of published guides may be obtained by request indicating the divisions desired to the U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Director of Regulatory Standards. Comments and suggestions for improvements in these guides are encouraged and should be sent to the Secretary of the Commission, U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Chief, Public Proceedings Staff.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust Review
10. General

wax. Similarly, for some currently available seals, such as lead seals, emphasis is placed on the difficulty of obtaining replicas of crimping tools and on the inability of unauthorized persons to obtain seals from the manufacturer. However, in sophisticated modern seals, the emphasis is on the unique identification characteristics (fingerprint) of the seal..

Function of a Sealing System

Seals are devices which are applied at convenient places to detect tampering and entry. Sealing systems consist of the seals themselves and the sets of procedures, techniques, and devices used in procuring, storing, and fingerprinting the seals; selecting the point of application; applying, removing, and identifying the seals; and judging whether entry or tampering has occurred.

The objective of utilizing a sealing system is to provide a level of assurance that no tampering or entry occurred during the period that the seal was applied. The degree of confidence in a seal system will vary directly with the effort required to defeat the seal and inversely with the motivation for defeating it. If the scheme used by a would-be diverter of the contents requires undetected tampering with the sealed object, the seal will present an added obstacle for the diverter which will require him to undertake extra activities. The chance that he will make a mistake and be detected is therefore increased.

An intangible effect of a sealing system is the psychological one of informing would-be diverters that security measures are being taken, thus deterring acts by weakly motivated people.

Limitations of Sealing System

The methods of attack on sealing systems that are potentially the most successful are those exploiting weaknesses of parts of the sealing system other than the seal itself. Although a sealing system would fail at the seal if the seal could be opened and reclosed without leaving any identifying marks that would indicate tampering, this would be difficult even in the case of lead seals which are normally considered relatively unreliable. Opening and closing the seal without leaving marks is difficult because of work hardening of the lead. Seals of a more sophisticated type are virtually impossible to open without leaving some indication of tampering.

A sealing system that depends on a lack of availability of blanks to the adversary can fail if the supplier of the seals or one of his employees can be persuaded to produce a set of replicas. This also presupposes a weakness in the method of identification used in the sealing system. In recognition of this problem, all manufacturers of seals make the point in their sales literature that precautions are taken to prevent delivery of unauthorized orders of blanks.

Sealing systems that depend on a lack of availability of blanks can also fail if it is possible to steal blanks from the storage area. Again, this presupposes some weakness in the identification method.

A sealing system can fail if new seals are not properly protected. Assume that an inspector brings a supply of seals previously fingerprinted at the home office. A diverter replaces some of the seals with forgeries, which the inspector, not having fingerprinting capability in the field, unsuspectingly installs in the plant. The diverter breaks the forged seals, gains access to the protected material, and applies the good seals previously stolen from the inspector. The inspector later removes the seals and sends them to the home office for the post-mortem examination that certifies their identity.

A sealing system can fail in the method of fingerprinting if the type and detail of information about the seal taken and recorded at the time of application are inadequate to make forgery by a diverter unattractive. In the case of sealing systems using lead seals, the fingerprinting is normally restricted to markings made at the time of application by means of the engraved dies of the sealing press. Such a die can be reproduced from an old seal. Another method of defeating any fingerprinting system is to substitute false records of fingerprints in the files of the sealing agency.

The selection of the point of application of the seal in a sealing system can lead to weakness if the containment membrane is not tamperproof. For instance, sealing the door of a truck might be useless if access can be gained by unbolting the door at the hinges.

The method of post-mortem examination of the seal can lead to failure of the system if the examination is not sufficiently thorough. A complete examination of the removed seal is required if the seal is to serve fully in the detection of tampering.

A sealing system can fail if the ways the seals are applied make them vulnerable to accidental damage since a history of such incidents might be used to conceal a few willful attacks. In particular, some seals used on shipping containers can be easily damaged during normal handling. In some cases plant operators request advance authorization to break some seals in emergency situations when inspectors will not be available to witness the operations. In either case, an inspector could be facing a broken seal, a plausible explanation, and some unsafeguarded material.

Types of Seals Commercially Available

Some types of security seals are being made in large numbers and have found use in industry for tamperproofing such things as utility meters, tanks of bonded liquor, and oil wells. These seals vary widely in reliability, and the simpler ones probably will not find an application in safeguarding nuclear materials. A brief description of some types of seals follows.

Lead Seal. Various types of lead seals are in common use. Essentially, a lead seal consists of a small block of lead with holes for the passage of the sealing wire. The wire is passed through the closure hasp on the container and then through the holes in the lead, which is then compressed so as to embed the wire.

Self-Locking Padlock Seal (Plastic). This seal uses an elastic wire which passes through the hasp and is inserted in a plastic block shaped in such a way that, once the wire springs into position, the wire cannot be removed without tearing or deforming the plastic.

Notched Metal Seal. This seal is a metal strip which is notched. The strip is passed through the hasp and bent at the notch. To remove the seal requires bending the metal strip at the notch again which results in breakage.

Self-Locking Padlock Seal (Steel). This seal is a sturdy lock-type seal. A U-shaped shackle is passed through the hasp and is then inserted into a steel block; expansion rings inside the block fall into grooves in the shackle ends when the shackle is properly seated.

Wire Lock Seal. This seal uses a serrated wire that is passed through the hasp and whose ends are inserted into holes in a metal box with spring teeth locking onto the serrations of the wire.

Boxcar Seal. This type is the typical railroad boxcar seal employing a metal strap which is passed through the hasp. Both pads of the strap are locked together inside a metal box at the time of closure.

Type E Seal. This seal consists of two metallic parts that, when snapped together, form a closed box about the knot on the wire passing through the hasp.

Pressure-Sensitive Seal. This seal has paper or plastic backing on one surface of which is a layer of adhesive. After proper application, this type of seal is difficult to remove without an indication that tampering has occurred.

Seals for Use in Safeguarding of SNM

Of the seals commercially available, three are sufficiently reliable for use in safeguarding SNM. These seals are (1) the pressure-sensitive seal, (2) the steel padlock seal, and (3) the type E seal.

The pressure-sensitive seal recommended for use in onsite storage of SNM is described in Regulatory Guide 5.10.

The steel padlock seal is a one-time padlock seal that is destroyed when removed. The most secure design at present appears to be the one requiring a hammer to drive a hardened steel shackle into a steel block. This seal is very rugged and may have use in some situations where accidental damage may be likely and where a lock is also needed.

The type E seal is a seal in which a fingerprint may be artificially created by scratches inscribed on the inside surfaces of the seal. The scratches are photographed before application of the seal. Later, at the container inspection point, the seal is removed and sent to a laboratory for analysis and comparison with the original photograph. The seal is destroyed in the examination. A disadvantage is the undesirable time lapse in getting the seal to the laboratory for the post-mortem examination and in getting the report back to the custodian who removed the seal.

The type E seals when fingerprinted are considered high-security seals. Defeating the seal by forgery would require accurate reproduction of internal surface details to such a degree that differences would not be distinguishable in a macrophotographic comparison. Defeating the seal by surreptitious attack would require penetration and repair techniques that would not be visibly evident under microscopic examination of the surfaces. The seal could be defeated by cutting and rejoining the wire without leaving marks. However, the use of multistrand wire makes unnoticeable rejoining difficult. At present, there appears to be no known form of attack by which the type E seal when fingerprinted can be defeated.

Other seals based on fiber optics and on cast plastics using photographic fingerprints are under development but not in common use. In general, such systems involve a field assembly and check of the fingerprint. Further development and evaluation are needed before they can be recommended.

C. REGULATORY POSITION

1. The three types of security seals identified below are generally acceptable to the Regulatory staff for use in protection and control of SNM:

a. Pressure-sensitive seals as described in Regulatory Guide 5.10, "Selection and Use of Pressure-Sensitive Seals on Containers for Onsite Storage of Special Nuclear Materials."

b. Padlock seals. These seals should be made of hardened steel that is capable of resisting cutting by a hacksaw. The shackle and the block should each carry a serial number.

c. Type E seals. The brass crown-like clasping device of this type of seal should be soldered to the brass top of the cylindrical cup. The bottom of the cylindrical cup should be copper. The interior surfaces of the cup, top and bottom, should have a unique fingerprint applied. The wire passing through the hasp of the enclosure to be sealed should be a stainless steel aircraft cable. This cable is fabricated of a minimum of nineteen strands of wire.

2. An acceptable sealing system should include the following considerations:

a. The outer surface of a seal should carry a serial number and the name or initials of the organization using the seal. The lettering and numbering should be readable and should be engraved, molded, punched, or otherwise applied in a way that prevents removal or changing of the numbers without leaving apparent damage. The seals should be sequentially numbered with sufficient alphameric or numeric symbols to prevent duplication of numbers in use at that facility.

b. A seal should be applied to a container in a manner that ensures that the contents cannot be removed from the sealed enclosure without destroying the seal or breaking into the enclosure. A seal should be applied immediately after the samples and data to identify and measure the contents have been taken.

c. The design and construction of a seal should ensure that disassembly and reassembly of the seal result in apparent residual indications of tampering detectable by the post-mortem examination techniques recommended for the seal.

d. A seal should be resistant to or be protected against the effect of the environment or rough treatment which would be detrimental to the seal components and would destroy any indications of tampering.

e. Seals should be available to and applied and removed by only designated individuals responsible to material control and accounting management. Removed seals should be disposed of in a manner to prevent reuse.

f. Precise records of each and all seals by serial number should be kept and, after application, should include data on the sealed contents. Such records should include dates and times of application and removal of the seals, the signatures of the individuals responsible to material control and accounting management for the data and for applying and removing the seal, and any discrepancy that is observed in the sealed contents.

g. Written procedures should be prepared covering the control, application, documentation, and post-mortem examination of seals. If the post-mortem examination is made by a person other than the custodian removing the seal, procedures should be established to maintain the chain of custody of the removed seal.

h. Samples of every batch of seals received from a seal supplier should be retained for future reference and comparison in case of detected tampering.

January 1974

U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.20

TRAINING, EQUIPPING, AND QUALIFYING OF GUARDS AND WATCHMEN

A. INTRODUCTION

Section 73.50 of 10 CFR Part 73, "Physical Protection of Plants and Materials," requires fuel reprocessing licensees and persons licensed to possess certain specified quantities of special nuclear material (SNM), respectively, to provide trained and equipped guards and watchmen to physically protect their facilities and to protect the SNM in their possession against theft. Further, §§ 73.30 through 73.36 of 10 CFR Part 73 require certain shipments of SNM to be accompanied by guards as escorts. This guide provides criteria acceptable to the Regulatory staff for a program for training, equipping, and qualifying guards and watchmen.

B. DISCUSSION

Guards and watchmen responsible for the protection of SNM onsite and in transit and for the protection of the facility against industrial sabotage should, like other components of the physical security system, meet minimum levels of performance and reliability. The licensee should assure that those responsible for security are capable, and qualified to execute the duties prescribed for them. Performance and reliability of the guard force can be assured by strict adherence to a program of:

1. Preemployment screening,
2. Training and qualification, and
3. Testing and requalification.

Preemployment screening provides a means to determine whether a prospective security employee is trustworthy and capable of performing the security tasks that will be assigned to him.

Training and qualification of guards and watchmen are necessary to assure knowledge of the facility licensee's or transport licensee's (transporter) [1] security plan and to assure a thorough understanding as to exactly what is and what is not expected of each guard and watchman. Further, the legal responsibilities and limitations involved in the execution of his duties should be made clear to every guard and watchman. Special emphasis should be given to the bearing and use of firearms.

Testing and requalification is needed to ensure the continued performance and reliability of guards and watchmen as components of the security system.

The licensee should provide all guards and watchmen training with regard to the details of the security plan they are expected to follow. The specific physical and training requirements of each guard and watchman will depend upon the duties charged to that guard or watchman.

The Commission's regulations make the following distinction between guards and watchmen: guards are armed and uniformed and have protection of SNM against theft and/or the protection of plant against industrial sabotage as their primary duty; watchmen,

[1] For the purposes of this guide, a transport licensee, or transporter, is any person who is licensed pursuant to the regulations of 10 CFR Part 50 or 70 who imports, exports, transports, delivers to a carrier for transport, or takes delivery free on board at the point where it is delivered to a carrier, special nuclear material, and who is subject to the requirements for the physical protection of special nuclear material in transit of 10 CFR Part 73.

who may or may not be armed and uniformed, protect the plant and the SNM therein in the course of other duties. For the purpose of this guide, the term watchman will refer to an individual who is never armed, and a third category, patrol watchman, will be considered as an arms qualified individual who may be issued arms during an emergency or threat situation and whose primary duty, at least during an emergency or threat situation, is the protection of the plant and the SNM therein.

For material shipments, armed escorts and armed monitors are considered guards, and unarmed escorts are considered patrol watchmen.

C. REGULATORY POSITION

A program acceptable to the Regulatory staff for the preemployment screening, training, testing, equipping, and qualifying of licensee security personnel should include the following:

1. Preemployment Screening

a. Minimum Qualification

Preemployment screening should be designed to assess the suitability of an applicant for consideration as a member of the licensee's security organization. The following are minimum qualifications:

(1) Minimum age of 21,

(2) Minimum education, high school diploma or equivalent,

(3) No record of felony convictions,

(4) General good health as determined by a physician prior to employment.

b. Employment Application

An employment application should be used to provide a basis for the screening process. The application should contain the following information:

(1) Full name,

(2) Date and place of birth,

(3) Citizenship,

(4) Current residence,

(5) Prior residences (past 5 to 10 years),

(6) Educational background (institutions, dates),

(7) Previous employment history (full adult life) including supervisors, employment function, reason for termination,

(8) Military service,

(9) Record of criminal convictions.

c. Physical Capabilities

(1) All security personnel should be capable of arduous physical exertion and be able to withstand exposure to unusual or inclement weather,[2]

(2) All security personnel should have vision correctible to 20/20 (Snellen) in each eye,

(3) All security personnel should have hearing loss not exceeding 30 dB in both ears, or 35 dB in the poorer ear, relative to normal hearing,

(4) All security personnel should be mentally alert and capable of understanding and performing the duties assigned.

d. Contract Service

If the licensee chooses to use a contract guard service, he should accept only security personnel who have undergone preemployment screening and who meet the qualifications prescribed above.

2. Training

Prior to assignment of security duties, each guard, watchman, and patrol watchman, whether hired by the licensee or provided by a contract service, should successfully complete a training program consisting of the following:

a. General training as outlined in Appendix A of this guide,

b. Training specific to the facility or transport licensee's security plan for normal, emergency, and threat situations as outlined in Appendix B of this guide.

3. Testing and Requalification

Each guard, watchman, and patrol watchman should be tested and requalified according to the following schedule:

a. Facility or transport security plan: general duties and responsibilities of security personnel–annually,

b. Facility or transport security plan: specific duties and responsibilities as assigned–semiannually,

c. Communication equipment and security equipment as appropriate–semiannually,

d. Arms qualification for guards and patrol watchmen (Appendix C)–semiannually,

e. Medical examination–annually.[3]

4. Equipment

The facility licensee, transporter, or contract service should issue uniforms, firearms, communication devices, and other security equipment as appropriate. Inspections

---

[2] United States Army Regulation AR 40-501, "Standards of Medical Fitness," offers a guide to the determination of an individual's physical ability to perform the duties of a guard or patrol watchman.

[3] Prior to reassignment to duty, a physician should certify the general good health of any guard, watchman, or patrol watchman returning for service after a prolonged illness.

should be conducted and documented by the security supervisor of the facility or transporter or by another individual designated by the licensee at least quarterly to assure proper care and condition of said equipment.

a. As a general practice, uniforms issued to guards and uniformed watchmen and patrol watchmen should be markedly distinct from those of local law enforcement authorities.

b. On-duty guards should be armed with sidearms of not less than caliber .38. Weapons should be kept loaded at all times while being carried by guards.

c. Weapons such as shotguns, rifles, riot guns, tear gas, and mace should be available and issued to guards and patrol watchmen as necessary. Such weapons should be loaded only upon issue, and should remain loaded for as long as they are carried by the guards or patrol watchmen.

d. Guards and watchmen on patrol should carry radio communication devices. An intercom or other means should be used to provide communication in areas of the facility where direct radio communication is not possible.

e. Fixed-site security organizations should be provided with at least one dedicated vehicle, such as a jeep, equipped with two-way radio communication for the purpose of quick response to intrusion or to an alarm. If the patrol area is so large that only patrol by vehicle is practical, at least one other dedicated vehicle should be provided. In addition to radio communication, vehicles used for response to intrusion or for armed escort of SNM shipments should be equipped with a loaded shotgun or riot gun, extra rounds of ammunition, flares, spare batteries for communication devices, spotlights, a CO_2 or dry powder fire extinguisher, and a first aid kit.

APPENDIX A

GENERAL TRAINING PROGRAM

This appendix lists topics and suggested time allotments for a 10-day general training program for guards and watchmen. The program is divided into two sections: points of law and security skills. The section on points of law is not intended to be a course in all aspects of the law, but rather is intended to introduce the guards and watchmen to, and familiarize them with, some essential principles of law of which the guards and watchmen should have a basic understanding in order to assist and protect them in the proper performance of their duties. Hence, the topics listed in that section should be covered in sufficient depth to assure that each guard, watchman, and patrol watchman possesses an understanding of (1) the general limits of legal authority of a private security guard as provided by State statutes and the common law, (2) the differences between a felony and a misdemeanor insofar as that difference affects his authority, (3) the permissible legal extent of a search and seizure as affected by his suspicion of a crime and by his actual witness of a crime, (4) the evidence generally necessary to prove the commission of a crime and particularly the importance of the preservation of "real evidence," and (5) the use of force legally permissible in self defense or in prevention of a crime involving property. The section on security skills should be directed at enabling security personnel to (1) perform their security duties in an effective manner, (2) effectively cooperate with other security personnel (including Federal, State, or local law enforcement authorities) responding to a request for assistance, and (3) effectively defend themselves and others, if necessary.

The program need not be limited to the topics listed herein, and other subjects may be included.[4] Reasonable latitude is expected to enable the licensee to develop his training program to best suit his needs. When formulating and implementing his training program, the licensee should consult with and obtain the advice of State and local law enforcement authorities.

SCOPE

The general training program should be adequate to help assure that the licensee's guards and watchmen are capable of providing protection of the facility against sabotage or SNM from theft, either in transit or at a fixed site, until the arrival of assistance from law enforcement authorities. The following potential sources of threats should be considered in the training program:

a. Lone individuals familiar with the construction and operation of the facility or the routing of vehicles transporting SNM.

b. A group of several individuals, some of whom may be armed with weapons such as rifles, sidearms, and explosives.

c. A group of unarmed individuals engaged in disorderly conduct or mob activities.

TOPICS

The following is a list of topics which should be presented, with suggested corresponding time allotments, in the 10-day training program. This list is not intended to be all inclusive nor is any recommendation made as to the order of presentation.

Points of Law

For this part of the training program to be successful, the legal concepts in this section of the program should be directly related to, and discussed in the narrow context of, the duties that guards, watchmen, and patrol watchmen are expected to perform. It is suggested that approximately three days (24 hours) of the 10-day program be devoted to discussion of the topics listed below:

Role of Law Enforcement .... 1 hour

A brief history of the development of law enforcement, division of legal authority (e.g., Federal, State, and local), and law enforcement ethics.

Legal Phrases and Definitions .... 2 hours

An explanation of the meanings and legal significance of the most commonly used legal phrases that a guard or watchman is likely to encounter.

Crimes and Elements .... 3 hours

Common law and/or statutory elements necessary for establishing certain specific crimes (e.g. assault, assault and battery, burglary, breaking and entering, larceny, receiving stolen property, carrying a concealed weapon, robbery).

[4] The licensee is referred to the recommendations contained in the "Private Police Training Manual" prepared and published by the Ohio Peace Officer Training Council in conjunction with the Attorney General of the State of Ohio. The licensee should evaluate the peculiarities of his own operation and determine whether additional topics should be included in his training program.

Laws of Arrest (Criminal Laws) .... 4 hours

A discussion of the legal authority to make arrests (without a warrant), probable cause, due process, rights of the accused, and other constitutional guarantees. Discussion should emphasize amount of force permissible when making arrest and situations where State law justifies use of "killing force."

Rules of Evidence .... 4 hours

Brief instruction in the fundamental concepts and rules of evidence, generally what is admissible and what is inadmissible in court as evidence, and methods of preserving real evidence.

Search and Seizure ... . 4 hours

An introduction to laws, rules, and methods of lawful search and seizure specifically as they pertain to private security guards and watchmen.

Techniques and Mechanics of Arrest .... 4 hours

Basic police techniques and methods used to make proper arrests and safe searches.

Examination .... 2 hours

An examination should be given at the completion of this section. A passing grade should be established as one of the requirements for satisfactory fulfillment of the course.

Security Skills

Approximately seven days (56 hours) of the 10-day training program should be devoted to the following practiced security skills:

Self Defense .... 16 hours
(for guards and patrol watchman)

A discussion of defensive weapons and methods of defending oneself against attack. Up to six hours of physical training should be included.

First Aid .... 8 hours

Basic first aid techniques in emergency situations. American Red Cross Standard Course should be taught.

Response to Crimes in Progress .... 3 hours

Descriptions of the proper action to be taken upon observing or being notified of a crime in progress.

Patrol Procedures .... 4 hours

A discussion of functional patrol procedures and methods in private property patrol, both on foot and by vehicle.

Crowd and Mob Control .... 4 hours

Crowd control problems frequently faced by special officers. State and Federal laws and court rulings as well as police handling and control.

Firearms Training .... 16 hours
(for guards and patrol watchman)

Firearms training for those who are armed while on duty should be required in addition to the basic training course. Training should include weapons familiarization, weapons safety, and range firing of revolvers and shotguns.

Firemanship .... 3 hours

A brief training period discussing the methods of fire safety, fire prevention, and fire control.

Examination .... 2 hours

An examination should be given at the completion of this section. A passing grade should be established as one of the requirements for satisfactory fulfillment of the course.

APPENDIX B

FACILITY OR CARRIER TRAINING PROGRAM

This appendix lists topics and suggested time allotments for a 5-day (3-day for transporter guards) program of training specific to the duties and responsibilities of guards, watchmen, and patrol watchmen under the facility or carrier security plan.

SCOPE

Training with respect to the licensee's security plan should be adequate to ensure that the licensee's guards and watchmen are fully aware of the duties and responsibilities charged to them under normal operating conditions, emergency conditions, and threat situations. It should be emphasized and clearly understood by every member of the security organization that under threat situations the primary responsibility of the licensee's security organization is to provide protection until the arrival of assistance from local law enforement authorities.

The training program should emphasize that guards and armed patrol watchmen are not to display or discharge their weapons, but are to keep their weapons in their holsters and are not to withdraw and discharge their weapons except in situations when such conduct would be permitted under the law of the State in which the facility is located or under the law of the State through which the vehicle transporting special nuclear material is traveling.

At no time should a guard or armed patrol watchman fire a "warning shot" into the air or ground. Warnings should be given verbally. Above all, it should be stressed to the guards the vital importance to the public health and safety and to the common defense and security of the United States that the unauthorized removal of special nuclear material from the facility or vehicle transporting the special nuclear material or the industrial sabotage to the facility be prevented.

TOPICS

Security Overview .... 3 hours
(2 hours for transporter escorts)

A discussion of the objectives of security plan, details of security organization structure, and command responsibility.

Records and Reports .... 3 hours
(2 hour for transporter escorts)

Detailed description of licensee procedures for completing status, inspection, tour, and other appropriate routine and special reports.

Facility Alarm System .... 8 hours
(Fixed site guards and watchmen)

Discussion of intrusion alarms used at the facility, their operation, location, and testing procedures. Explanation of the alarm testing schedules. Field demonstrations of alarm equipment.

SNM Transport Vehicles .... 1 hour
(Transporter escorts)

A description of the vehicles used to transport SNM and of the methods of packaging SNM for shipment.

Communication Equipment .... 1 hour

Operation and routine testing of communications devices used by the licensee.

Routine Procedures .... 8 hours
(Fixed site guards and watchmen)

A variety of topics should be covered; among them are: identification checks; badges and badging procedures; detection equipment used by licensee; vital areas, what they contain, why they are vital; escort procedures within protected area; personnel and package searching procedures; patrol and inspection procedures.

Emergency Procedures .... 4 hours
(Fixed site guards and watchmen)

Fire and criticality evacuation procedures, location of fire equipment, and security procedures under emergency conditions.

Emergency Procedures .... 3 hours
(Transporter escorts)

Security procedures following a vehicle accident.

Routine Procedures .... 3 hours
(Transporter escorts)

Discussion of check-in procedures, detour policy, and shift-change procedures (long hauls).

Threat Situations .... 3 hours

Types of credible attack and expected response. Procedures for calling for assistance: who to call, when, what information is to be given.

Use of Firearms .... 2 hours

Proper use of firearms during threat situations emphasizing permissible use of force in various situations.

Radiological Safety .... 5 hours

Areas where SNM is found at the facility, type and form of the SNM stored, processed, or transported, and identifying characteristics of SNM containers. Provisions of the Commission's regulations for the protection of personnel against exposure, health problems associated with exposure, precautions and procedures to minimize exposure, and proper handling procedures for SNM.

Examination .... 3 hours
(2 hours for transporter escorts)

Supervision

In addition to the above topics, training should include up to six weeks of on-the-job supervision.

APPENDIX C

ARMS QUALIFICATION PROGRAM

Guards, and other individuals who may be issued arms during a threat situation (e.g., patrol watchmen), should qualify semiannually on one of the following courses:

SHORT COURSE

Range	Type Fire	Time	No. Shots	No. Strings	Target	Maximum Points
25 yd	Slow	5 min	5	2	25 yd (SF)	100
25 yd	Timed	20 sec	5	2	25 yd (TF)	100
25 yd	Rapid	10 sec	5	2	Silhouette	100

Target Specifications:*

25 yd (SF)--21 in. x 24 in. with No. 7, 8, 9, and 10 rings black and black area 5.50 in. diameter (B-16).

25 yd (TF)--21 in. x 24 in. with No. 9 and 10 rings black and black area 5.54 in. diameter (B-8).

Silhouette -- B-27

Guards must achieve a minimum point total of 175.

* As set forth by the National Rifle Association in its Official Rules and Regulations.

NATIONAL POLICE COURSE

Firing Stages:

a. **Seven-Yard Course:** Twelve shots double action from the crouch position. Time starts with gun in holster and includes reloading for second six shots. Time allowed: 25 seconds.

b. **Twenty-Five-Yard Course:** Six shots kneeling, double action; six shots standing, double action, left hand from behind barricade; six shots standing, double action, right hand from behind barricade. Time allowed: 90 seconds.

c. **Fifty-Yard-Course:** Six shots sitting, six shots prone, six shots left hand police standing from behind barricade, and six shots right hand from behind barricade single action. Time allowed: 2 minutes and 45 seconds.

d. **Twenty-Five-Yard Course:** Six shots standing without support, single action. No barricade or other support is used. Time allowed: 12 seconds.

Target Specifications:* B-27 Target

Guards must achieve a minimum percentage score of 70%.

In addition, guards and patrol watchmen should be instructed in the use of mace or tear gas if provided by the licensee or contract service.

June 1974

U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.27

SPECIAL NUCLEAR MATERIAL DOORWAY MONITORS

A. INTRODUCTION

Paragraph (b), "Exit Requirement," of §73.60, "Additional Requirements for the Physical Protection of Special Nuclear Material at Fixed Sites," of 10 CFR Part 73, "Physical Protection of Plants and Materials," requires that individuals exiting from material access areas be searched for concealed special nuclear material (SNM). This guide describes means acceptable to the Regulatory staff for employing SNM doorway monitors to comply with that requirement.

B. DISCUSSION

Special nuclear material doorway monitors provide an efficient, sensitive, and reasonably unobtrusive means of searching individuals exiting from a material access area for concealed SNM. With proper installation and operation, gram quantities or less of SNM can be detected with a high level of reliability while maintaining a low false alarm rate.

1. Theory of Operation

The doorway monitor is composed of a detector unit(s), associated electronics, and alarm logic. The detector unit(s) is sensitive to the radiations which emanate from the SNM and responds to these radiations (usually gamma rays) by generating current pulses. These pulses are amplified, filtered, and fed to alarm logic which interprets the number (or rate) of pulses in some period of time, for example, one second. The alarm logic may be either a digital or analog system; in either case, if the number (or rate) of pulses exceeds a set level, an alarm condition ensues.

2. General Characteristics

Typically, the detectors of a doorway monitor are NaI(Tl) scintillators or solid or liquid organic scintillators. Geiger-Mueller detectors have also been used in this application, although the lower intrinsic efficiency of these detectors renders them less suitable than scintillation detectors.

Detectors are arranged such that a detection area is defined by a plane perpendicular to the line of passage of individuals through the doorway monitor. Various arrangements of the detectors are possible; however, specific placement of detectors is usually dictated by the need to eliminate dead spots.

Some commercially available doorway monitors are equipped with an automatic background updating system. The automatic background updating system periodically monitors and averages the background. A doorway monitor equipped with an automatic background updating system is also provided with a treadle pad or beam-break system to indicate that the sensitive area is occupied. When the sensitive area is occupied, the radiation level detected by the doorway monitor is compared with the mean background. If the level is "significantly" greater than the mean background, an alarm condition ensues. Significance is usually determined by comparing the radiation level when the sensitive area is occupied with the mean background plus some multiple of the square root of the mean background*

*The square root of the mean of a Poisson-distributed quantity is the unbiased estimate of the standard deviation of that quantity.

USAEC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the AEC Regulatory staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Published guides will be revised periodically, as appropriate, to accommodate comments and to reflect new information or experience.

Copies of published guides may be obtained by request indicating the divisions desired to the U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Director of Regulatory Standards. Comments and suggestions for improvements in these guides are encouraged and should be sent to the Secretary of the Commission, U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Chief, Public Proceedings Staff.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust Review
10. General

Thus the condition for an alarm can be written as

$$G > B + n\sqrt{B},$$

where B is the mean background, G is the radiation level with the sensitive area occupied, and n is a multiplier, usually an integer between 4 and 10.* The value of n directly affects the false alarm rate, and the combination of B and n affect the sensitivity.

Although the automatic background updating system allows unattended use of the doorway monitor, for technical reasons, the system may be less effective in certain situations. Techniques to prevent this are described in the Regulatory Position.

Doorway monitors not equipped with an automatic background updating system either must rely on the inherent sensitivity of the instrument and low background variation to ensure that concealed SNM will be detected or must be attended so that a measurement of background can be taken immediately prior to use and the alarm level set to maintain the desired sensitivity to concealed SNM. As with the doorway monitor equipped with an automatic background updating system, a doorway monitor not so equipped compares the activity with the detection area occupied with some set value, usually the measurement of background taken just prior to use. In any case, the expression above can be used as a condition of alarm by replacing $B + n\sqrt{B}$ with the set level.

Whether or not a doorway monitor is equipped with an automatic background updating system, high background activity will decrease sensitivity. Measuring activity for longer periods will somewhat compensate for high background; however, longer measurement periods will make use of the doorway monitor less convenient.

C. REGULATORY POSITION

1. **Minimum Qualifications for SNM Doorway Monitors**

a. General

(1) SNM Doorway monitors should be used in conjunction with a metal detector and should be installed in a passageway (see Regulatory Guide 5.7, "Control of Personnel Access to Protected Areas, Vital Areas, and Material Access Areas,") in such a manner that objects cannot be passed over, around, or under the detection area.

(2) The detector elements should be designed and positioned so that detection sensitivity is as uniform as possible over the detection area; in no case should any areas where SNM is not detectible be permitted.

(3) Power, sensitivity, and other controls of the doorway monitor should be tamper-safed when unattended.

(4) Signal lines connecting alarm relays to the alarm monitor should be supervised.

(5) Some doorway monitors may require an individual to occupy the detection area for a specified time, longer than a normal walking pace would provide. If this is the case, the doorway monitor should be provided with a treadle pad and a "clock" device to assure that the detection area is occupied for the requisite time. An aural and visual indication should be given if an individual being searched does not occupy the area sufficiently long.

b. System Specification

(1) *Plutonium-239.* A doorway monitor used to detect plutonium should be capable of detecting a minimum of 0.5 gram of plutonium-239 encased in a minimum of 3 mm of brass at a 90% confidence limit. The false alarm rate should be less than 0.1% (Appendix C).

(2) *Uranium-233.* A doorway monitor used to detect uranium-233 should be capable of detecting within 4 hours of purification* a minimum of 1 gram of uranium-233 containing between 7 and 10 ppm of uranium-232 encased in a minimum of 3 mm of brass at a 90% confidence limit. The false alarm rate should be less than 0.1% (Appendix C).

(3) *Uranium-235.* A doorway monitor used to detect uranium-235 should be capable of detecting a minimum of 3 grams of uranium-235 contained in uranium enriched to 20% or more in the uranium-235 isotope encased in a minimum of 3 mm of brass at a 50% confidence limit. The false alarm rate should be less than 0.1% (Appendix C).

2. **Use of Doorway Monitors**

In general, doorway monitors should be used in locations of minimum background and minimum background fluctation. If circumstances dictate use of a doorway monitor in an area of high background, sufficient shielding should be provided to maintain necessary sensitivity.

a. Attended Doorway Monitor

(1) If the doorway monitor is attended during use, it need not be equipped with an automatic

*Note that, in general, for a count rate system, the condition for alarm should be modified to account for the response time of the instrument as follows:

$$G > B + n\sqrt{B}(1 - e^{-t/\tau})$$

where t is the counting time and τ is the time constant of the instrument. If, as should be the case, $t/\tau > 5$ the added factor is essentially unity.

*Purification means removal of all decay products.

background updating system, although such capability is preferred.

(2) Prior to each use* of a doorway monitor not equipped with an automatic background updating system, a measurement of background should be taken, and the alarm threshold should be set to the proper value listed in Table I for the measured background and the proper n value as determined in Appendix B. Each individual to be checked should, in turn, enter the detection area and be required to remain sufficiently long for the device to operate properly. During use, the background should be checked and the alarm threshold reset at least each 15 minutes.

(3) With the individual being checked in the detection area, an alarm should sound if the activity in the detection area exceeds the alarm threshold T, as such a situation would indicate the presence of SNM.

(4) The doorway monitor should be equipped with a high-background alarm which will sound if the measurement of background exceeds the appropriate maximum permissible background level listed in Table II as determined in Appendix C. The doorway monitor should not be used during such periods of high background.

b. Unattended Doorway Monitor

(1) If the doorway monitor is unattended, an automatic background update system should be incorporated into the doorway monitor electronics and alarm logic. The control circuitry, if possible, should be located at the central alarm station (or other monitoring point).

(2) Door interlocks and closed-circuit TV in combination with beam breaks, motion detectors, and/or treadle pads, should be employed to:

(a) Indicate to the person manning the central alarm station that an individual has entered the secure access passageway and/or is approaching the doorway monitor,

(b) Allow observation of the individual approaching the doorway monitor,

(c) Preclude a slow approach to the sensitive area of the doorway monitor, and

*By use is meant an individual or several individuals, each, in turn, being checked for SNM by the doorway monitor. The maximum period between threshold sets while the doorway monitor is in use is determined by the stability of local background and may necessarily be more frequent than every 15 minutes.

(d) Activate the electronics and alarm logic when an individual is within the detection area and initiate operation of the doorway monitor.

(3) An alarm should sound in the central alarm station if, when occupied, the activity in the detection area exceeds the internally set threshold level (the mean background plus some multiple times the square root of the mean background), as such a situation would indicate the presence of SNM upon the individual being checked.

(4) The doorway monitor should be equipped with a high-background alarm which will sound if the average background at the location of the doorway monitor exceeds the appropriate maximum permissible background level listed in Table II as determined in Appendix C. The doorway monitor should not be used during such periods of high background. Other monitored exits should be used.

3. **Testing and Calibration**

a. Testing

Doorway monitors should be tested by passing an appropriate source of the amount and isotope specified in Regulatory Position C.1.b. through the doorway monitor no less frequently than once per day.* In addition, a functional performance test should be carried out at least once per week. An acceptable functional performance test procedure is discussed in Appendix A of this guide

b. Calibration

Doorway monitors should be calibrated with a source of the amount, configuration, and variety of SNM to be detected (e.g., 0.5 gram Pu in 3 mm of brass). Calibration should be carried out according to a procedure such as that in Appendix B.

c. Operating Instructions

Operating instructions should be posted near the doorway monitor, if attended, or at the monitoring point if the doorway monitor is unattended. The instructions should clearly indicate the procedure for use of the doorway monitor and the procedure for setting thresholds, if appropriate. In addition, the operating instructions should indicate what corrective action is to be taken and who is to be notified in the event of a malfunction.

*Doorway monitors used to search for concealed U-233 should be tested according to §6 of Appendix A.

TABLE I

ALARM THRESHOLD

				T			
B	n = 4	5	6	7	8	9	10
100	140	150	160	170	180	190	200
120	164	175	186	197	208	219	230
140	187	199	211	223	235	246	258
160	211	223	236	249	261	274	286
180	234	247	260	274	287	301	314
200	257	271	285	299	313	327	341
220	279	294	309	324	339	353	368
240	302	317	333	348	364	379	395
260	324	341	357	373	389	405	421
280	347	364	380	397	414	431	447
300	369	387	404	421	439	456	473
320	392	409	427	445	463	481	499
340	414	432	451	469	488	506	524
360	436	455	474	493	512	531	550
380	458	477	497	516	536	555	575
400	480	500	520	540	560	580	600
420	502	522	543	563	584	604	625
440	524	545	566	587	608	629	650
460	546	567	589	610	632	653	674
480	568	590	611	633	655	677	699
500	589	612	634	657	679	701	724
520	611	634	657	680	702	725	748
540	633	656	679	703	726	749	772
560	655	678	702	726	749	773	797
580	676	700	724	749	773	797	821
600	698	722	747	771	796	820	845
620	720	744	769	794	819	844	869
640	741	766	792	817	842	868	893
660	763	788	814	840	866	891	917
680	784	810	836	863	889	915	941
700	806	832	859	885	912	938	965
720	827	854	881	908	935	961	988
740	849	876	903	930	958	985	1012
760	870	898	925	953	981	1008	1036
780	892	920	948	975	1003	1031	1059
800	913	941	970	998	1026	1055	1083
820	935	963	992	1020	1049	1078	1106
840	956	985	1014	1043	1072	1101	1130
860	977	1007	1036	1065	1095	1124	1153
880	999	1028	1058	1088	1117	1147	1177
900	1020	1050	1080	1110	1140	1170	1200
920	1041	1072	1102	1132	1163	1193	1223
940	1063	1093	1124	1155	1185	1216	1247
960	1084	1115	1146	1177	1208	1239	1270
980	1105	1137	1168	1199	1230	1262	1293

TABLE I (Cont'd)

ALARM THRESHOLD

T

B	n = 4	5	6	7	8	9	10
1000	1126	1158	1190	1221	1253	1285	1316
1200	1339	1373	1408	1442	1477	1512	1546
1400	1550	1587	1624	1662	1699	1737	1774
1600	1760	1800	1840	1880	1920	1960	2000
1800	1970	2012	2055	2097	2139	2182	2224
2000	2179	2224	2268	2313	2358	2402	2447
2200	2388	2435	2481	2528	2575	2622	2669
2400	2596	2645	2694	2743	2792	2841	2890
2600	2804	2855	2906	2957	3008	3059	3110
2800	3012	3065	3117	3170	3223	3276	3329
3000	3219	3274	3329	3383	3438	3493	3548
3200	3426	3483	3539	3596	3653	3709	3766
3400	3633	3692	3750	3808	3866	3925	3983
3600	3840	3900	3960	4020	4080	4140	4200
3800	4047	4108	4170	4232	4293	4355	4416
4000	4253	4316	4379	4443	4506	4569	4632
4200	4459	4524	4589	4654	4718	4783	4848
4400	4665	4732	4798	4864	4931	4997	5063
4600	4871	4939	5007	5075	5143	5210	5278
4800	5077	5146	5216	5285	5354	5424	5493
5000	5283	5354	5424	5495	5566	5636	5707
5200	5488	5561	5633	5705	5777	5849	5921
5400	5694	5767	5841	5914	5988	6061	6135
5600	5899	5974	6049	6124	6199	6273	6348
5800	6105	6181	6257	6333	6409	6485	6562
6000	6310	6387	6465	6542	6620	6697	6775
6200	6515	6594	6672	6751	6830	6909	6987
6400	6720	6800	6880	6960	7040	7120	7200
6600	6925	7006	7087	7169	7250	7331	7412
6800	7130	7212	7295	7377	7460	7542	7625
7000	7335	7418	7502	7586	7669	7753	7837
7200	7539	7624	7709	7794	7879	7964	8049
7400	7744	7830	7916	8002	8088	8174	8260
7600	7949	8036	8123	8210	8297	8385	8472
7800	8153	8242	8330	8418	8507	8595	8683
8000	8358	8447	8537	8626	8716	8805	8894
8200	8562	8653	8743	8834	8924	9015	9106
8400	8767	8858	8950	9042	9133	9225	9317
8600	8971	9064	9156	9249	9342	9435	9527
8800	9175	9269	9363	9457	9550	9644	9738
9000	9379	9474	9569	9664	9759	9854	9949
9200	9584	9680	9775	9871	9967	10063	10159
9400	9788	9885	9982	10079	10176	10273	10370
9600	9992	10090	10188	10286	10384	10482	10580
9800	10196	10295	10394	10493	10592	10691	10790

TABLE II

MAXIMUM PERMISSIBLE BACKGROUND $\alpha = 0, \quad P_\alpha = 50\%$

B

G	n = 4	5	6	7	8	9	10
100	67	61	55	50	46	42	38
120	83	76	70	64	59	54	50
140	100	92	85	78	72	67	62
160	117	108	100	93	86	80	74
180	134	124	116	107	100	93	87
200	151	141	131	123	114	107	100
220	168	157	147	138	129	121	113
240	186	174	163	153	144	135	127
260	203	191	180	169	159	150	141
280	221	208	196	185	174	165	155
300	238	225	213	201	190	179	170
320	256	242	229	217	205	194	184
340	274	259	246	233	221	210	199
360	292	277	263	249	237	225	214
380	310	294	280	266	253	240	229
400	328	312	297	282	269	256	244
420	346	329	314	299	285	272	259
440	364	347	331	316	301	287	274
460	382	365	348	332	317	303	290
480	400	382	365	349	334	319	305
500	418	400	383	366	350	335	321
520	436	418	400	383	367	351	337
540	455	436	417	400	383	367	352
560	473	454	435	417	400	384	368
580	491	471	452	434	417	400	384
600	510	489	470	451	433	416	400
620	528	507	488	468	450	433	416
640	546	525	505	486	467	449	432
660	565	543	523	503	484	466	448
680	583	562	541	520	501	482	464
700	602	580	558	538	518	499	481
720	620	598	576	555	535	516	497
740	639	616	594	573	552	532	513
760	657	634	612	590	569	549	530
780	676	652	629	607	586	566	546
800	695	671	647	625	603	583	563
820	713	689	665	643	621	600	579
840	732	707	683	660	638	617	596
860	750	725	701	678	655	633	613
880	769	744	719	695	673	650	629
900	788	762	737	713	690	667	646
920	806	780	755	731	707	685	663
940	825	799	773	748	725	702	679
960	844	817	791	766	742	719	696
980	863	835	809	784	760	736	713

TABLE II (Cont'd)

MAXIMUM PERMISSIBLE BACKGROUND $\alpha = 0$, $P_\alpha = 50\%$

B

G	n = 4	5	6	7	8	9	10
1000	881	854	827	802	777	753	730
1200	1069	1039	1009	981	953	926	900
1400	1258	1225	1193	1161	1131	1101	1073
1600	1448	1412	1377	1343	1310	1278	1247
1800	1638	1600	1563	1527	1491	1457	1423
2000	1829	1789	1749	1710	1673	1636	1600
2200	2020	1978	1936	1895	1855	1816	1778
2400	2212	2167	2124	2081	2039	1998	1958
2600	2404	2357	2312	2267	2223	2180	2138
2800	2596	2548	2500	2453	2407	2363	2318
3000	2789	2738	2689	2640	2593	2546	2500
3200	2982	2929	2878	2828	2778	2730	2682
3400	3175	3121	3068	3016	2964	2914	2865
3600	3368	3312	3258	3204	3151	3099	3048
3800	3561	3504	3448	3392	3338	3284	3232
4000	3755	3696	3638	3581	3525	3470	3416
4200	3949	3888	3829	3770	3713	3656	3600
4400	4143	4081	4020	3960	3900	3842	3785
4600	4337	4273	4211	4149	4088	4029	3970
4800	4531	4466	4402	4339	4277	4216	4155
5000	4725	4659	4593	4529	4465	4403	4341
5200	4919	4852	4785	4719	4654	4590	4527
5400	5114	5045	4977	4910	4843	4778	4713
5600	5309	5238	5169	5100	5032	4966	4900
5800	5503	5432	5361	5291	5222	5154	5087
6000	5698	5625	5553	5482	5411	5342	5274
6200	5893	5819	5745	5673	5601	5531	5461
6400	6088	6012	5938	5864	5791	5719	5648
6600	6283	6206	6130	6055	5981	5908	5836
6800	6478	6400	6323	6247	6172	6097	6024
7000	6673	6594	6516	6438	6362	6286	6212
7200	6868	6788	6709	6630	6552	6476	6400
7400	7064	6982	6902	6822	6743	6665	6588
7600	7259	7176	7095	7014	6934	6855	6777
7800	7455	7371	7288	7206	7125	7045	6965
8000	7650	7565	7481	7398	7316	7234	7154
8200	7846	7760	7674	7590	7507	7425	7343
8400	8041	7954	7868	7782	7698	7615	7532
8600	8237	8149	8061	7975	7889	7805	7721
8800	8433	8343	8255	8167	8081	7995	7911
9000	8628	8538	8449	8360	8272	8186	8100
9200	8824	8733	8642	8553	8464	8376	8290
9400	9020	8928	8836	8745	8656	8567	8479
9600	9216	9122	9030	8938	8848	8758	8669
9800	9412	9317	9224	9131	9039	8949	8859

TABLE II (Cont'd)

MAXIMUM PERMISSIBLE BACKGROUND α = 1.3, P_α = 90%

B

G	n = 4	5	6	7	8	9	10
100	57	51	46	42	38	34	31
120	72	65	59	54	49	45	41
140	87	80	73	67	62	57	52
160	103	95	87	81	75	69	64
180	119	110	102	95	88	81	76
200	135	126	117	109	101	94	88
220	151	141	132	123	115	107	100
240	168	157	147	138	129	121	113
260	185	173	163	153	143	135	127
280	201	189	178	168	158	149	140
300	218	206	194	183	172	163	154
320	235	222	210	198	187	177	167
340	252	239	226	214	202	191	181
360	270	255	242	229	217	206	196
380	287	272	258	245	233	221	210
400	304	289	275	261	248	236	224
420	322	306	291	277	263	251	239
440	339	323	308	293	279	266	254
460	357	340	324	309	295	281	268
480	374	357	341	325	311	297	283
500	392	374	357	342	326	312	298
520	409	391	374	358	342	327	313
540	427	409	391	374	358	343	329
560	445	426	408	391	374	359	344
580	463	443	425	407	391	375	359
600	480	461	442	424	407	390	375
620	498	478	459	441	423	406	390
640	516	496	476	457	439	422	406
660	534	513	493	474	456	438	421
680	552	531	511	491	472	454	437
700	570	549	528	508	489	470	453
720	588	566	545	525	505	487	469
740	606	584	562	542	522	503	485
760	624	602	580	559	539	519	500
780	642	619	597	576	555	535	516
800	660	637	614	593	572	552	532
820	679	655	632	610	589	568	549
840	697	673	649	627	605	585	565
860	715	690	667	644	622	601	581
880	733	708	684	661	639	618	597
900	751	726	702	679	656	634	613
920	770	744	720	696	673	651	630
940	788	762	737	713	690	668	646
960	806	780	755	731	707	684	662
980	824	798	773	748	724	701	679

TABLE II (Cont'd)

MAXIMUM PERMISSIBLE BACKGROUND $\alpha = 1.3$, $P_\alpha = 90\%$

G	n = 4	5	6	7	8	9	10
1000	843	816	790	765	741	718	695
1200	1027	997	968	940	913	887	861
1400	1212	1180	1148	1117	1088	1059	1030
1600	1398	1363	1329	1296	1264	1232	1201
1800	1586	1548	1512	1476	1441	1407	1374
2000	1773	1734	1695	1657	1620	1584	1548
2200	1962	1920	1879	1839	1800	1761	1724
2400	2151	2107	2064	2022	1980	1940	1900
2600	2340	2294	2249	2205	2162	2119	2078
2800	2530	2482	2435	2389	2344	2300	2256
3000	2720	2670	2622	2574	2527	2481	2435
3200	2911	2859	2808	2759	2710	2662	2615
3400	3101	3048	2996	2944	2894	2844	2795
3600	3292	3238	3183	3130	3078	3027	2976
3800	3484	3427	3371	3317	3263	3210	3158
4000	3675	3617	3560	3503	3448	3393	3340
4200	3867	3807	3748	3691	3634	3577	3522
4400	4059	3998	3937	3878	3819	3762	3705
4600	4251	4188	4126	4066	4006	3946	3888
4800	4443	4379	4316	4253	4192	4131	4072
5000	4636	4570	4505	4442	4379	4317	4256
5200	4828	4761	4695	4630	4566	4502	4440
5400	5021	4953	4885	4819	4753	4688	4624
5600	5214	5144	5075	5007	4940	4874	4809
5800	5407	5336	5266	5196	5128	5061	4994
6000	5600	5528	5456	5386	5316	5247	5180
6200	5793	5720	5647	5575	5504	5434	5365
6400	5987	5912	5838	5765	5692	5621	5551
6600	6180	6104	6029	5954	5881	5808	5737
6800	6373	6296	6220	6144	6070	5996	5923
7000	6567	6488	6411	6334	6258	6184	6110
7200	6761	6681	6602	6524	6447	6371	6296
7400	6955	6874	6794	6715	6636	6559	6483
7600	7148	7066	6985	6905	6826	6747	6670
7800	7342	7259	7177	7096	7015	6936	6857
8000	7536	7452	7369	7286	7205	7124	7044
8200	7731	7645	7561	7477	7394	7313	7232
8400	7925	7838	7753	7668	7584	7501	7419
8600	8119	8031	7945	7859	7774	7690	7607
8800	8313	8225	8137	8050	7964	7879	7795
9000	8508	8418	8329	8241	8154	8068	7983
9200	8702	8611	8521	8433	8345	8257	8171
9400	8897	8805	8714	8624	8535	8447	8360
9600	9091	8998	8906	8815	8725	8636	8548
9800	9286	9192	9099	9007	8916	8826	8737

APPENDIX A

PROCEDURE FOR TESTING SNM DOORWAY MONITORS FOR FUNCTIONAL PERFORMANCE

Doorway monitors should be tested by employing a test source of the same isotope of SNM the doorway monitor is used to detect as follows:

1. With the detection area unoccupied, measure and record background.

2. Determine alarm threshold T from Table I (see Appendix B).

3. Place a test source in the detection area of the doorway monitor. The test source should be such that the activity in the detection area slightly exceeds the T level.* The doorway monitor should go into an alarm condition if operating properly.

4. Remove test source to its original location and measure background once again. If the measurement of background taken immediately after the test varies by more than $2\sqrt{B}$ from the background taken before the test, the test should be repeated, for such a difference indicates nonrandom fluctuations of the background or equipment malfunction. The probability of such an occurrence due to the randomness of the background is less than 8%.

5. A calibration source (Appendix B) should be carried repeatedly to various places within the detection area of the doorway monitor in simulation of actual use to verify that the SNM can be detected everywhere within the detection area and to assure proper operation of treadle pads, beam-break, or similar devices if the doorway monitor is so equipped.

6. Doorway monitors used to search for concealed uranium-233 should be tested with each uranium purification run, but no more frequently than daily. The test source should be freshly purified uranium-233 (within four hours of removal of decay products).

*The test source may be improvised by partially shielding the calibration source.

APPENDIX B

PROCEDURE FOR DETERMINING MAXIMUM PERMISSIBLE BACKGROUND

Background should be measured over several workshifts to determine the setpoints for alarm threshold (with or without automatic background updating) to assure that normal operation will be minimally affected by alarms due to high background.

The doorway monitor should be calibrated with the amount of the appropriate isotope specified in Regulatory Positions C.1.b(1), (2), or (3) of this guide (e.g., 0.5 gram plutonium-239 in 3 mm of brass).

The calibration procedure described below is essentially a means of determining maximum permissible background for effective operation of the doorway monitor.

1. Place a calibration source variously about the detection area and take readings to determine the least sensitive point. This location of minimum sensitivity should be maintained as the calibration point.

2. Measure background over several workshifts to determine the periods of high background and the range of background. A minimum of 20 measurements should be taken. The variance of the background is given by

$$\text{Var B} = \frac{1}{N-1} \sum_{i=1}^{N} (B_i - B)^2 \qquad (1)$$

where N is the number of measurements, B is the mean of the background measurements, and B_i is the i^{th} background measurement.

3. With the calibration source at the calibration point, the mean gross counts G should be determined during a period of high background to establish the upper operating range of the doorway monitor. Table II lists various maximum permissible background levels for a given value of G for values of the parameters n and α. During periods when the background exceeds the value found from Table II, the sensitivity of the doorway monitor will generally be below that specified as minimum in Regulatory Position C.1.b of this guide.

The parameter n is a function of the background variation and the permissible false alarm rate and is calculated from

$$n \geqslant 3.1 \left(\frac{\text{Var B}}{B} \right)^{1/2} \qquad (2)$$

Generally, n is taken as an integer. If n satisfies the above expression, the expected false alarm rate (Appendix C) due to background fluctuations should be less than 0.1%. Larger values of n will decrease the expected false alarm rate; however, the maximum allowable background for a given G will also decrease.

4. For doorway monitors equipped with automatic background updating systems, the alarm threshold is

$$\text{Counts} > B + n\sqrt{B}, \qquad (3)$$

where n should be derived from expression (2), and the instrument set accordingly.

5. The high-background alarm should be set at the B value given in Table II for the measured G and calculated n values.

6. For doorway monitors not equipped with an automatic background update, the value of n determined above should be employed in the use of the doorway monitor according to Regulatory Position C.2.a.

---

*The false alarm rate is estimated by the probability that an observation of a quantity distributed normally about some value X will exceed X by n(Std. deviation of X). The factor 3.1 limits the false alarm rate to 0.1%, while the factor $(\text{Var B/B})^{1/2}$ compensates for observed deviations in the background distribution from Poisson.

APPENDIX C

DETECTION CONFIDENCE LIMITS, THRESHOLDS, AND MAXIMUM PERMISSIBLE BACKGROUND

With a calibration source at the calibration point, the condition for an alarm is, in general,

$$g > T = B + m\sqrt{\text{Var } B} \qquad (1)$$

where g is a single measurement of G (the mean radiation level with the source), B is the mean background, and m is some multiplier. The detection confidence limit is the probability that with the calibraiton source at the calibration point, any single determination of G will exceed a threshold T, i.e., the above inequality will be satisfied. For any given probability P_α, there exists a value α such that

$$g > G - \alpha\sqrt{\text{Var } G} \qquad (2)$$

with a probability of P_α, where g is any single measurement of the quantity G. Hence the condition for a detection confidence limit of P_α is

$$G - \alpha\sqrt{\text{Var } G} > T = B + m\sqrt{\text{Var } B}. \qquad (3)$$

For a given value of G, solving (3) gives the maximum permissible B at which the doorway monitor will detect the source with a confidence P_α. For P_α = 90%, α = 1.3, and for P_α = 50%, α = 0.

The condition for a false alarm* is written as

$$b = B + \beta\sqrt{\text{Var } B} > T \qquad (4)$$

where b is a single measurement without the source and β is a number corresponding to a false alarm probability P_β. For P_β = 0.1%, β = 3.1. Hence the necessary condition for maintaining a false alarm rate below P_β is

$$b = B + \beta\sqrt{\text{Var } B} < B + m\sqrt{\text{Var } B}. \qquad (5)$$

However, the doorway monitor actually compares b with $B + n\sqrt{B}$, hence the condition on n becomes

$$\beta\sqrt{\text{Var } B} < m\sqrt{\text{Var } B} = n\sqrt{B} \qquad (6)$$

or

$$n > \beta\left(\frac{\text{Var } B}{B}\right)^{1/2}. \qquad (7)$$

In Table I threshold values of T were determined by substituting equation (6) into equation (3):

$$T = B + n\sqrt{B}$$

The values of B in Table II were then calculated for α = 1.3 and α = 0 from equation (3) assuming that, for the determination of G, the background should be reasonably stable and therefore $\sqrt{\text{Var } G} \sim \sqrt{G}$.

*False alarm means an alarm condition generated by statistical fluctuations in the background radiation or by instabilities of the electronics which appear as background fluctuations when the detection area is occupied.

June 1974

U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.30

MATERIALS PROTECTION CONTINGENCY MEASURES FOR URANIUM AND PLUTONIUM FUEL MANUFACTURING PLANTS

A. INTRODUCTION

Sections 73.40, "Physical Protection: General Requirements at Fixed Sites," and 73.50, "Requirements for Physical Protection of Licensed Activities," of 10 CFR Part 73, "Physical Protection of Plants and Materials," prescribe requirements for the physical protection of special nuclear materials (SNM) and the plants in which they are used or stored. Section 70.22, "Contents of Applications," of 10 CFR Part 70, "Special Nuclear Material," requires, among other things, that each application for a license to possess certain quantities of special nuclear material (SNM) contain a full description of the applicant's program for control of and accounting for SNM which will be in his possession under license and a physical security plan for meeting the physical protection requirements of 10 CFR Part 73. Section 70.51, "Material Balance, Inventory, and Records Requirements," requires, among other things, that certain licensees establish, maintain, and follow written material control and accounting procedures which are sufficient to enable the licensee to account for the SNM in his possession under license. Proposed §70.58, "Fundamental Nuclear Material Controls," would require, if adopted, that each licensee who is authorized to possess certain quantities of SNM establish material balance areas or item control areas for the physical and administrative control of nuclear material.

Essential to the protection of special nuclear material against theft are proper planning, implementation, and testing of measures designed to provide protection of special nuclear material even under emergency or other nonroutine conditions. This guide describes measures acceptable to the Regulatory staff for assuring continued protection of special nuclear material in such instances.

B. DISCUSSION

1. Scope of Materials Protection Contingency Measures

The basic philosophy of this guide to the establishment of design and operational measures for the protection of SNM under nonroutine conditions is that, since no system is immune to malfunction, backup measures should be provided to maintain the level of protection afforded by each of the normal materials protection systems. Further, since emergencies or nonroutine situations may not follow anticipated patterns, such backup measures should provide flexibility to accommodate a variety of possible failure modes. For example, to provide adequate protection capability in the event of power failure, equipment malfunction, or guard incapacitation, the contingency measures should include, respectively, an alternative source of power, redundant hardware, and additional support personnel.

Protection of the plant against industrial sabotage that could endanger the public health and safety by exposure to radiation is beyond the scope of this guide, although some of the measures identified herein may provide protection against such acts as well. In addition, emergencies that may pose a threat to plant security or personnel health and safety but not to the protection of SNM are also beyond the scope of this guide. Emergencies that may be caused or utilized by a thief to conceal the removal (either previous or concomitant) of SNM, however, are considered.

2. Objectives of Emergency Materials Protection Measures

During emergencies, the effectiveness of normal security measures for protecting SNM may be reduced.

Any emergency that requires complete or partial evacuation of a material access area because of health and safety considerations may result in a necessary relaxation of exit control requirements. The possibility of evacuation procedures deleteriously affecting the protection of SNM can be minimized by proper planning and posting of emergency procedures and by a program of instruction and drills for personnel at the facility.

It also is possible that routine accountability measures for protecting SNM may be compromised by the sudden and unexpected movement, removal, or alteration of SNM or SNM records. Effective emergency measures that replace or supplement routine materials protection measures and are implemented in accordance with established emergency planning procedures can enhance the protection of materials in the following manner:

a. The likelihood of theft will be reduced. Measures taken to limit access to SNM and to provide surveillance over an area in which an emergency situation exists will tend to deter an individual from engaging in unauthorized or illegal acts.

b. Theft of special nuclear material can be detected. Emergency and postemergency measures can control and document the movement, removal, or alteration of SNM and the quantities involved.

c. The amount of damage to or accidental loss of SNM may be reduced, thereby further improving the likelihood that a theft will be detected. Emergency materials protection measures for locating and identifying an emergency condition, transmitting emergency information to responsible individuals, and taking actions necessary to protect material can minimize the extent of damage to or accidental loss of SNM.

d. The capability for recovering stolen material is improved. Emergency monitoring and postemergency assay and accountability measures can help to reconstruct the event, thereby aiding recovery of material.

e. If potential nonroutine conditions are thoroughly considered in the initial planning and established emergency operating measures are followed, a facility can be operated under certain nonroutine conditions without jeopardizing the protection of SNM.

3. Definitions

For the purpose of this guide, the following definitions are provided:

a. NONROUTINE EVENT means any condition that alters the approved features of a facility, the equipment, or the method of operation such that the requirements for materials protection are threatened or are not being met. For example, a power outage, damage to records, equipment malfunction, guard incapacitation, or a change in equipment and plant structure that leads to a reduction in the capability to protect SNM can each represent a functional loss of part of the required materials protection system.

b. EMERGENCY MEASURES are those provisions that are taken to protect SNM in response to a nonroutine event. In addition, emergency measures include nonroutine measures taken to prevent the degradation of conditions that could result in a reduction or loss of materials protection if not controlled or if left untreated. Postemergency measures are taken to protect and account for SNM following events during which its protection may have been compromised.

c. NATURAL EVENT means a condition that results from natural causes such as severe weather conditions, floods, and earthquakes.

d. NUCLEAR EVENT means a condition resulting from a nuclear accident such as the sudden release of radiation (as in a criticality incident).

e. OPERATIONAL EVENT means a condition resulting from fire, equipment failure, injury to personnel, release of and contamination from SNM or other radioactive material following a spill or process malfunction, false alarm, or the functional loss of part of the materials protection system.

4. Emergency Materials Protection System

An emergency materials protection system, as with any security system, consists of detection, communication, and response elements (human or automatic), which together constitute a workable system. The failure or any one of these elements to function constitutes a system failure.

Warning of an impending or imminent emergency can be obtained from (1) detection measures based on sensors that automatically activate alarms or otherwise alert individuals that an emergency exists, (2) instruments that monitor normally varying conditions, and (3) surveillance of emergency indicators by either remote devices or direct observation. Such warning could include indications of severe weather conditions, processes that are out of control with respect to temperature or pressure, buildup of SNM approaching criticality limits, or the release of radioactive materials. Appropriate sensors may detect among other things, radiation, temperature changes, motion, interruption or alteration of an electric current, and electromagnetic changes. An emergency also may be detected by remote observation with the aid of closed-circuit television (CCTV) monitors or by direct observation by an individual at the scene.

When an existing or imminent emergency condition is detected, individuals responsible for taking appropriate actions must be notified. The actions taken by security personnel, plant management, and employees at the time of an emergency depend on the alarms and information that are transmitted to them. Emergency instructions and actions usually are based on signal transmissions by wire or radio to visible and audible annunciating (warning) devices. Warnings and instructions also may be relayed during an emergency by direct voice communication.

The objectives of the response or emergency actions taken by individuals to deal with an emergency are, in order of priority, (1) to protect the health and safety of the general public and of individuals at the plant, (2) to assure overall security and protection of materials, (3) to assure that all SNM is accounted for, and (4) to reestablish routine materials protection procedures as soon as possible.

In protecting the safety and lives of individuals, measures taken to evacuate personnel, administer first aid, and protect personnel from radiation hazards also can help to protect SNM. The rapid deployment of the guard force and other emergency security personnel can assure continued materials protection during and following an emergency. Emergency actions by an emergency supervisor and by trained technical support personnel can assure a rapid assessment of the location, condition, and amount of SNM affected by the emergency, thereby aiding postemergency actions and the resumption of routine materials protection procedures.

5. Temporary Operation Under Nonroutine Conditions

Following a natural, operational, or nuclear event that results in a temporary loss of part of a materials protection system, it may be desirable to continue operation (cleanup, production in unaffected areas, etc.) of the facility on a temporary basis, provided the facility or equipment is properly designed to accommodate emergency measures adequate for the protection of material during such periods. Operating in such a condition also might be desirable during periods of plant construction, alteration, or equipment changes.

Whenever a system functions under conditions for which it was not designed, the possibility of component malfunction increases. In such cases a system failure can be averted by a fail-safe design and by proper action of individuals.

Nonroutine conditions may occur as a result of modification of process equipment and plant design, changes in operating or maintenance procedures, or the temporary loss of portions of the materials protection system (detection, communication, or response element).

Some nonroutine operating conditions may not be recognized as emergencies. However, any loss of capability to protect SNM requires immediate remedial measures if the materials are to be provided with continued protection.

Identification of appropriate contingency measures can be aided by consideration of the following nonroutine conditions:

a. Functional loss of SNM isolation measures such as access control devices for materials processing or storage areas or remotely operated process or storage handling equipment.

b. Need for access by maintenance, installation, or construction personnel not authorized to have access to SNM and not normally permitted to work in a materials access area.

c. Reduced capability to inspect or test for compliance with requirements for processing, storing, transferring, measuring, or protecting SNM. This could be a result, for example, of process or equipment changes or relocation.

d. Compromise of keys, locks, or combinations to locks that are used to secure SNM or SNM accountability records.

e. Functional loss of personnel or package searching devices installed at passage points in the physical barriers.

f. Failure of remote surveillance equipment.

g. Unavailability of dock facilities normally used for isolating shipments and receipts of SNM or for isolating SNM from other materials.

h. Failure of the intrusion alarm protection system.

i. Loss of offsite communication capability at the central alarm station.

j. Commingling of SNM assigned to different material balance areas (MBAs) as a result of loss of identification or undocumented movement of SNM-bearing materials.

k. Loss of automatic data processing capability for control and accounting of SNM:

1. Reduced vault storage capacity that may be caused, for example, by a spill of radioactive material.

The materials protection measures that would apply to nonroutine operations are emergency substitutes for normal requirements. Operation under these measures are intended to proceed only during a temporary loss of routine protection capability.

C. REGULATORY POSITION

Backup or special measures and actions that can be taken to help assure the continued protection of SNM during an emergency or threatened emergency are described below. For each component of the normal materials protection system the failure mode that may result from fire, explosion, criticality, or contamination (either accidental or deliberate) should be identified. To provide protection, the backup measure for each system component should be invulnerable to the event that caused the failure of that component.

Emergency materials protection measures that affect activities in material access areas may, in some, cases, impact on necessary safety measures. If prescribed emergency materials protection measures (e.g., evacuation to a supervised assembly area or surveillance of rescue vehicles) would place individuals in further jeopardy, health and safety considerations[1] take precedence. Further, if prescribed materials protection measures are less stringent than other requirements (as, for example, health and safety requirements or local building codes) the more stringent requirements should apply.

1. Detection Aids

The following guidelines constitute measures acceptable to the Regulatory staff for detecting actual or potential conditions that would compromise routine materials protection measures.

a. Reports from offsite severe-weather warning or meteorological services should be used for predicting adverse weather conditions that could compromise materials protection. If a natural event that can jeopardize the protection of SNM is predicted, all SNM in process, to the extent practicable, should be placed in containers, sealed and locked in vaults, or located in other areas that will provide protection from theft and from physical damage that could reduce the effectiveness of postemergency procedures. (See also Regulation Position C.5, "Postemergency Materials Accountability Measures.")

b. Sensors should be installed to detect conditions of temperature, pressure, shock, release of radioactive materials, and interruption of vital services and equipment that could precipitate an emergency with a potential effect on the protection of SNM. (Although written for a different purpose, IEEE Standard 279-1971[2] contains useful guidance for the installation of sensors in Section 3, Items 3-6.)

[1]Other regulatory guides that deal with emergency plans to protect the health and safety of workers and the general public from accidental radioactivity releases are under development.

[2]IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." Copies may be obtained from the Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, New York 10017.

c. In the event of failure of a sensor or other instrumentation, parameters that had been monitored by the failed device should be visually monitored by direct or remote means unless a redundant sensor is available to monitor the parameter.

2. Communication Measures

The following guidelines constitute emergency measures that are acceptable to the Regulatory staff for transmitting warning or alert signals and for communicating during and after a reported emergency.

a. Signals that indicate when and where an emergency condition exists should be a fail-safe, tamper-resistant design and should include both visible and audible annunciating devices. Transmission and annunciator equipment should conform to Interim Federal Specification W-A-00450B(GSA-FSS) dated February 16, 1973, entitled "Alarm Systems, Interior, Security, Components For."[3]

b. Tamper-resistant annunciators should be located in at least two places within a material access area such that they can be seen and heard by supervisory and operating personnel whose actions may be needed to protect material or to avert an imminent emergency that could compromise the protection of material. Additional annunciators for all emergency signals should be located at the continuously manned central alarm station.

c. Onsite one-way communications consisting of a plant-wide public-address system and portable battery-powered megaphones should by available for relaying instructions to evacuating and evacuated personnel.

d. At the time of an emergency, telephone usage should be restricted to essential messages having to do with the emergency.

e. In addition to systems required for communication with local law enforcement authorities,[4] communication by telephone or radio should be available to notify key off-duty company personnel (to provide additional security, supervisory, technical support, or cleanup personnel, as needed to protect or account for SNM). A backup communication capability, e.g., designation of an offsite duty officer (supplied with company transportation) who would be contacted by the law enforcement agency, should be available for contacting key individuals in the event of a general telephone outage.

f. Security plans with local law enforcement agency authorities should provide for periodic "check-in" procedures and should assure that an inability of the

[3]Copies may be obtained from the Standardization Division, Federal Supply Service, General Services Administration, Washington, D.C. 20406.

[4]Paragraph 73.50(e)(3) of 10 CFR Part 73.

authorities to communicate with the continuously manned central alarm station will be treated by the authorities as a call for assistance. Contacts or liaison with local law enforcement authorities should include utilization of intelligence-gathering groups for possible warning or to aid in the recovery of stolen material.

3. Personnel Control

The following guidelines constitute emergency measures that are acceptable to the Regulatory staff for controlling access to SNM during or following an emergency.

a. Evacuation

(1) All personnel should be instructed and drilled in the salient features of the emergency materials protection plan. Since the plan may be quite complex and repetitive, an abstract, memo, manual, or list of rules should be published and distributed to all employees and visitors. In addition, key instructions for individual areas within the plant should be posted in conspicuous locations.

(2) If consistent with personnel health and safety considerations, emergency rendezvous areas should be located within the protected area.

(3) Personnel who are evacuated from a facility because of an emergency should leave according to established plans and routes with a minimum of travel through material access areas. Emergency exit routes from a material access area should avoid passage through other material access areas.

(4) Personnel evacuated from or through a material access area should be under surveillance wherever possible as they are being evacuated, should be kept under surveillance after they are evacuated, and should rendezvous at a single predetermined location until dismissed or instructed to return to work. Such personnel should be identified from area access control records and accounted for.[5]

(5) Emergency exits from the protected area should be designed to allow continuous visual surveillance of evacuating personnel during evacuation.

(6) Areas where individuals assemble following an evacuation should be clear of obstructions that would provide concealment such as buildings, fences, trees, or shrubbery and should be restricted from public access.

(7) All persons and vehicles leaving a protected area or emergency rendezvous area should be assumed to bear concealed SNM and should be accompanied by supervisory or security personnel until circumstances allow a search to be conducted.[5] Personnel requiring offsite medical attention should not be exempted.

(8) If an emergency situation cannot be controlled adequately with the available onsite manpower, additional off-duty company personnel should be called in or support should be obtained from offsite local, State, or Federal agencies. Offsite organizations may include local law enforcement authorities, fire departments, AEC personnel, State health departments, hospitals, and ambulance and rescue services.

b. Emergency Access Control

(1) Records of persons granted access to material access areas prior to, during, and after an emergency should be secured and maintained for later analysis.

(2) Measures should be taken to protect or provide backup for required intrusion detectors[6] so that all exits from and entrances to an evacuated material access area can be closed, locked, and alarmed. If not alarmed, such areas should be kept under continuous direct or remote visual surveillance.

(3) Construction materials should be available on site for making emergency repairs to breaks in the physical barriers.

(4) Access to evacuated material access areas should be restricted to authorize security, supervisory, emergency materials protection, and rescue personnel in accordance with established emergency procedures.

(5) Emergency keys or lock combinations necessary for emergency personnel should be stored in tamper-resistant, alarmed enclosures and should be changed whenever there is reason to believe such an enclosure may have been compromised. (Disadvantages of master keyed locks is discussed in another regulatory guide.[7])

c. Surveillance

(1) Emergency lighting from an alternative or secondary power source should be provided to all material access areas to provide illumination sufficient for surveillance[8] during periods when the normal lighting system is inoperative. If an area-wide power failure would disrupt the secondary power supply, battery-powered floodlights designed to activate automatically if the normal lighting system fails should be installed throughout the material access area in a manner that provides general illumination of not less than 0.2 foot-candle.[9] In addition, all security personnel should be provided with portable battery-powered spotlights. All battery-powered lights should be provided with a signal light to warn of weak batteries.

(2) Planning should include, as appropriate, the use of portable CCTV equipment to survey and to monitor activites in a material access area following an emergency in which sensors or other monitoring equipment have become inoperative and conditions exist that make extended occupancy hazardous.

[5] See also Regulatory Guide 5.7, "Control of Personnel Access to Protected Areas, Vital Areas, and Material Access Areas."

[6] Paragraph 73.60(c) of 10 CFR Part 73.

[7] Regulatory Guide 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Material."

[8] Regulatory Guide 5.14, "Visual Surveillance of Individuals in Material Access Areas."

[9] Local safety codes may require higher levels of illumination to assure safe evacuation.

(3) Additional security or guard personnel should be called in or other qualified plant personnel should be designated to support the regular security personnel as needed for performing backup guard functions, surveillance, and materials protection for a material access area that is threatened or affected by an emergency.

(4) All emergency vehicles (company-owned or owned by an offsite organization) that are brought into a protected area and are used for the transfer of equipment or personnel to or from a material access area during or following an emergency should be under continuous surveillance by supervisory or security personnel while within the protected area. If surveillance has not been continuous, exiting vehicles and any individuals therein should be accompanied until both can be searched for concealed SNM.

4. Nonroutine Operation

The following guidelines constitute measures that are acceptable to the Regulatory staff for assuring continued protection of SNM while a plant or process is temporarily operating under nonroutine conditions which could otherwise reduce the protection afforded by routine materials protection measures.

a. Necessary Nonroutine Operation

While certain nonroutine operations may be desirable (particulary cleanup after a natural or nuclear emergency), extensive use of emergency measures cannot justify long-term operation in noncompliance with AEC rules, regulations, license conditions, or orders.[10]

(1) The design of automated or remotely operated equipment for processing, transporting, or storing SNM should provide for access to equipment, as allowed by safety considerations, to facilitate removal or draindown of SNM. Manual operations or maintenance to equipment that may permit access to SNM should be performed within controlled material access areas by individuals authorized to have access to SNM.

(2) Material access areas should be designed with sufficient clearance to permit the installation of temporary physical barriers to isolate areas that might require postemergency cleanup or other nonroutine activities by personnel who are not authorized access to SNM. If deductive surveillance[11] is to be utilized for activities in such "isolated" areas, the area should be separated from other areas by barriers equivalent to those normally required for material access areas.[12]

(3) Where possible, SNM should be removed from process equipment and accounted for before any nonroutine activites are undertaken in that area. All hardware and tools removed from a material access area should be examined for SNM, and all personnel should be searched for concealed SNM.[13]

(4) To provide for temporary handling of both shipments and receipts of SNM in the same dock area, physical separation should be provided between the dock platforms and material storage areas at the dock. Storage areas should be designed with clear space sufficient to accommodate operations normally done on the dock e.g., removal of outer packaging, gross measurement check, seal verification, etc.

(5) Process equipment in which in situ measurements or in situ calibration of instruments is normally performed should be designed with provisions for emergency access and working space to utilize alternative or duplicate sampling, measuring, and calibrating equipment or devices.

b. Protection System Component Failure

Continuous direct visual surveillance by security or supervisory personnel or other backup measures should be provided for all materials security devices, the operability or required level of performance of which cannot be verified.

(1) Whenever changes in process operations, equipment design, or equipment location can reduce normal inspection and testing capability, special design features and operating procedures implemented must be consistent with approved license amendments.[14] To aid implementation and approval, duplicate or equivalent backup measuring and testing devices may be provided. Also, use of calibrated nondestructive assay equipment, or procedures which call for a partial shutdown for sampling, special calibration of instruments, or obtaining physical measurements, may be substituted for normal in-line or dynamic inventory measurements. Equipment also may be designed with supplemental viewing and inspection ports or openings that can take the place of primary access ports blocked owing to changes in equipment design or location.

(2) Provisions for manual searches or backup monitoring equipment should be available in the event of temporary malfunction of equipment routinely used to search individuals, packages, and vehicles exiting from material access areas. Equipment normally in use at two different control points may serve as backup for one another, provided either control point can be deactivated (blocked, locked, and alarmed) when not properly equipped.

(3) Backup equipment should be available for monitoring all waste streams for SNM. When not in use, this equipment should be stored in an area physically separated from primary monitoring equipment.

(4) Backup capability for surveillance of material processing or storage areas should be provided in the event of failure of an intrusion alarm or remote visual

[10] Paragraphs 70.32(c) and 70.32(e) of 10 CFR Part 70.

[11] See Regulatory Guide 5.14, "Visual Surveillance of Individuals in Material Access Areas."

[12] Paragraph 73.2(f) of 10 CFR Part 73. (Standards for Barrier Construction are the subject of a regulatory guide under development.)

[13] Paragraph 73.60(b) of 10 CFR Part 73.

[14] Paragraph 70.32(b) of 10 CFR Part 70.

surveillance system. This backup may be a redundant intrusion alarm system and/or a capability for continuous on-location visual surveillance by security or supervisory personnel who can communicate with the continuously manned central alarm station.

(5) Security, supervisory, or authorized operating personnel such as storage or vault custodians should provide continuous direct surveillance of any normally locked or secured process or storage area for periods when keys are lost or unaccounted for, locks are damaged, or lock combinations are compromised. This surveillance should be continued until all affected locks are replaced or until lock combinations are changed by authorized security or management personnel.[7]

5. Postemergency Materials Accountability Measures

The following guidelines constitute actions that are acceptable to the Regulatory staff for assuring continued materials control and accounting following an emergency.

a. Accounting

(1) Emergency measures should assure the integrity of material accountability records so that a valid postemergency material balance can be made following conditions in which the identification of SNM items may have been lost or obliterated, SNM may have been relocated to another material balance area (MBA) without adequate transfer records, or equipment that may have contained SNM has been removed.

When SNM has been relocated to another area, a temporary MBA should be established that encompasses both the original area and the new area. This temporary MBA should be physically identified with suitable markings or barriers. All SNM within the temporary MBA should be physically inventoried and new records obtained and reconciled with the preemergency records. Measurements should be of sufficient quality that the uncertainty of the postemergency inventory is no greater than the uncertainty of the preemergency records. New separate MBAs with material transfer stations, custodians, and records may be necessary for SNM (or equipment containing SNM) that is relocated for postemergency cleanup or recovery.

(2) If electronic data processing is used for SNM control and accounting, a master file should be maintained which can be updated from a log of transactions processed subsequent to the last updating of the file. A capability for the manual recording of data normally entered automatically may also be desirable.[15]

(3) As soon as possible after an emergency all SNM control records should be accounted for and placed in locked storage or kept under continuous direct or remote surveillance until needed for inventory and SNM accountability.

b. Control and Documentation

(1) Emergency exits should be designed so that they may be used temporarily to replace normal access or exit control points. Inoperative access points should be barricaded or locked and, in either case, they should be alarmed consistently with requirements for material access areas.[16] Direct visual surveillance should be maintained over any unalarmed, though inoperative or unused, access points (emergency as well as normal access points).

(2) Solid, liquid, and gaseous effluents from a material access area normally must be monitored to detect and measure SNM that may be released.[17] Retention ponds and tanks should be provided as necessary to allow monitoring of liquid effluents from emergency-related activities such as fire fighting and decontamination.

(3) The location of all SNM in a facility should be determined as soon as possible after an emergency to assure continued surveillance and access control of such material. Temporary material access areas or boundaries should be established in the event that SNM must be moved or barriers removed during or as a result of an emergency.

(4) Nondestructive assay equipment should be available to assist in timely verification of SNM content of materials that may have been spilled, moved, or altered during an emergency.

(5) If SNM that is not in process cannot be protected because of temporary loss of normal vault or storage capability, emergency measures should be taken to assure that security and accountability requirements are met. Temporary storage areas should be designated and should be physically separated from process or other material access areas with a temporary isolation barrier that can be kept under continuous direct surveillance by security personnel or by an authorized vault custodian. If other areas approved for SNM storage are available, material should be relocated to these areas and afforded the full protection routinely required of SNM (access control, intrusion alarms, surveillance, etc.). While SNM is being relocated to temporary storage, sealed containers should not be opened unless there is reason to suspect that seals have been compromised. Unsealed containers of SNM should be identified, sealed, and listed before being relocated. All relocated containers should be locked[7] (either individually or in a larger container with others) to physically isolate them from individuals who are authorized to have access to materials normally assigned to the temporary storage area. Similarly, SNM normally assigned to the area should be locked or otherwise protected from individuals who are authorized to have access to the relocated material.

[15] Regulatory guides dealing with material control and accounting records are under development.

[16] Paragraph 73.60(c) of 10 CFR Part 73.

[17] Paragraph 70.22(b)(1) of 10 CFR Part 70.

When normal vault or other storage capability has been restored and the material is returned from temporary storage, the integrity of each seal should be verified.[18]

(6) In the event the relocated SNM has not been continuously isolated while in temporary storage or if there is reason to suspect that a seal has been compromised, all suspect and unsealed packages at that storage location, whether believed to contain SNM or not, should be opened if necessary and the contents remeasured to verify that no SNM has been stolen or illicitly transferred to another container to aid later removal.

(7) All measures taken to protect SNM during an emergency, whether in accordance with established emergency plans or a departure from such plans, should be documented. This should include, where feasible, a record of instructions given and actions taken and should include interviews with individuals who were in the material access area immediately prior to the emergency. These records should be reviewed for post-accident or postemergency analysis of possible deliberate cause and for modifying emergency procedures as appropriate.

[18] Regulatory Guide 5.15, "Security Seals for the Protection and Control of Special Nuclear Material."

June 1974

U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.31

SPECIALLY DESIGNED VEHICLE WITH ARMED GUARDS FOR ROAD SHIPMENT OF SPECIAL NUCLEAR MATERIAL

A. INTRODUCTION

Paragraph 73.31(c) of 10 CFR Part 73, "Physical Protection of Plants and Materials," requires that road movements of special nuclear material (SNM) in quantities identified in §73.1(b)(2) be protected by one of the following methods: (1) shipment with at least two armed guards accompaning the shipment in a separate escort vehicle or (2) shipment in a specially designed truck or trailer which reduces the vulnerability to diversion by design features that permit immobilization of the van and provide barriers or deterrents to physical penetration of the cargo compartment. If armed guards are used with the specially designed vehicle, immobilization is not required. Paragraph 73.30(d), requires that the qualification of individuals to act as guards used pursuant to §73.31(c) be documented. This guide describes features acceptable to the Regulatory staff for a vehicle operated by armed guards to ship special nuclear material by road and for the qualification of the armed guards.

B. DISCUSSION

There are two approaches that can be taken to satisfy §73.31(c)(2), i.e., specially designed truck or trailer. One method would be the use of a specially designed secure cargo vehicle that is constructed so as to resist entry for a substantial period of time by unauthorized personnel using a wide variety of tools and weapons. The penetration time would be commensurate with the time needed for law enforcement agencies to respond to the scene of an emergency. The vehicle would be designed to be immobilized upon command in case of a diversion attempt.

The other method would be through the use of armored car service. In this case resistance to unauthorized entry is provided, in part, by the armed personnel within the vehicle who are in turn protected by the inherent design of the armored vehicle.

Acceptable characteristics of vehicles and personnel used in armored car service are provided in this guide.

1. ARMOR

Armored vehicles are supplied to the industry by a very small number of manufacturers. The specific design of the armor supplied by each company is considered proprietary information. The armor can generally be described with respect to its resistance to projectile penetration. All manufacturers provide armor which will resist initial penetration by bullets from readily available small arms. The armor is usually affixed to the vehicle in such a way as to provide protection to the occupants against attack from any external direction.

2. CAB-CARGO INTERFACE

The cab-cargo interface can be provided with several options. In most cases the separating wall between cab and cargo compartment is armored to provide protection in case either compartment is compromised. A window of bullet-resistant material which allows the crew in one compartment to have a clear view of the access doors of the other compartment is also provided. Some models have a door that allows passage from the cab to the cargo compartment without leaving the vehicle. Other models are equipped with gunports that permit firing from cab to cargo compartment.

3. GUARDS AND DRIVERS

Normally an armored vehicle crew consists of two or three individuals divided between the cab and cargo compartments. For long-distance trips the crew is often increased to allow rest periods for drivers and guards.

SNM shipments are expected to involve frequent long-distance trips of two or more days. In order to maintain the full protective capacity of the armored service during these trips, it is important that adequate crews for continuous manning of both compartments during normal operation be supplied. Considerable flexibility in achieving this end would be provided if both guards and drivers were qualified and permitted to perform either function (guard or driver).

4. DOOR LOCKS

All armored vehicles are supplied with compartment locks for both the cab and cargo doors. In many cases access to the cargo compartment requires positive action by personnel in both compartments when the cargo compartment is occupied by a guard.

5. ALARM SYSTEM

Many of the armored cars presently in service are equipped with audible alarms and/or flashing lights similar to those used by police and emergency vehicles. The awareness of attack that such alarms elicit in the general public can facilitate response to attack or recovery of diverted material.

6. SECURING OF CARGO

Armored cars have no standard provision for tying down cargo. This is understandable in view of the types of cargo normally handled by these carriers. For SNM cartage, where larger and heavier cargos can be expected, some provision for adequate tie-down restraint will be required to provide for cargo integrity and personnel safety. It is expected that only minor effort and expense would be required to equip existing vehicles with tie-down fittings.

7. RADIATION MEASUREMENTS

Each shipment will be configured at origin to be in compliance with Department of Transportation (DOT) general packaging and safety requirements (DOT regulation 49 CFR 173.393). Additionally, in order to monitor total radiation absorbed by personnel, some type of personnel dosimetry should be considered. Types of personnel dosimeters are the film badge and pocket dosimeter for gamma radiation, and the thermoluminescent neutron dosimeter (TLD) for neutron radiation. The film badge consists of a film packet in a plastic holder. The film badge or TLD provide an accurate indication of exposure to radiation over a long period of time. Since the film has to be developed and read on a densitometer, it may take some time to obtain a radiation reading. The pocket dosimeter, on the other hand provides a quick estimate of radiation received over a short period of time, but is not as accurate as the film badge for gamma radiation.

8. GAS PROTECTION

Many of the newer armored vehicles use a flow-through (front-to-back) air system for heating and cooling the vehicle interior. Typically, these systems draw outside air from the front (cab area) of the vehicle and expel exhaust air through vents in the upper areas of the vehicle. A slight positive internal pressure provided by the air system offers some resistance to the introduction of gaseous substances. The air intake is under occupant control and can be closed. Some vehicles are normally equipped with gas masks. The use of gas masks, filters, and internal air supplies for carriers of SNM would enhance the ability of vehicle crew members to resist gas attacks.

9. ANTENNA PROTECTION

Almost all armored vehicles are equipped with communication systems of some kind. Each vehicle is equipped by the purchaser of the vehicle although the manufacturer may provide mounting structures or access areas for the communication system components. In some instances, the purchaser may provide the communication equipment to the manufacturer who will install the equipment at the time the vehicle is constructed. Both radio and radiotelephone systems are in use. Each system is dependent on the use of radio signals received and transmitted from a vehicle-mounted antenna which could logically become the first target of an attack. Loss of an antenna during attack would preclude the vehicle occupants from either notifying external agents of the attack or from seeking aid or assistance. To provide for sufficient delay during an attack for a vehicle crew to transmit emergency messages, antenna protection is desirable. Such protection could be provided in the form of concealment, multiplicity, or hardening. The actual antenna could be concealed or designed to appear as some other object while conventionally appearing dummy antennas would be conspicuously located on the vehicle. Multiple antennas using internal switching could offer a delay sufficient to enable emergency messages to be transmitted. Hardened, attack-resistant antennas could be designed and used to provide a delay time. Combinations of these or other similar methods could enhance the viability of transmission.

C. REGULATORY POSITION

The characteristics listed below are acceptable to the Regulatory staff for a road vehicle operated by armed guards in order to comply with AEC regulations pertaining to SNM shipments. Additional Federal, State, and local requirements pertaining to safe interstate and local transport of cargo may also pertain to such shipments and compliance with these requirements is expected.

1. ARMOR

The vehicle should provide protection for the driver(s) and guard(s) against projectile impact. The external surface of the vehicle (side panels, floor, top, firewall area, and viewing areas) should be constructed of materials which are resistant to at least the muzzle impact energy of a .357 magnum bullet. The fuel tank(s) should also be provided with similar protection against projectile impact. The fuel tank(s) should be equipped with a lock-type cap and a screen in the tank nozzle to prevent the insertion of an explosive device into the tank.

2. CAB-CARGO INTERFACE

The wall separating the cab and cargo compartments should be armored. Additional features to be considered in the detailed construction of the cab-cargo interface depend on the method selected for the protection of the shipment. At least one of the methods listed below should be used. These methods are similar in that each provides the capability for the crew to use firearms to prevent entry into the cargo compartment without leaving the vehicle.

a. An armed guard should be permanently stationed in the cargo compartment. In this case, a continuous wall of armor with a bullet-resistant window would be considered adequate as a cab-cargo interface.

b. Access to the cargo compartment from the cab should be available so that a guard can go directly from the cab to the cargo compartment without leaving the vehicle.

c. Gunports should be available which will permit firing from the cab into the cargo compartment. Additionally, the gunports should permit firing of the weapon at wide angles so that overt entry from all sides of the cargo compartment can be prevented.

3. GUARDS AND DRIVERS

All personnel of an armored vehicle should be qualified to perform all normal operational tasks involved with a shipment. Both guards and drivers should be qualified to perform either function, and interchange of function should be allowed if required for the safety and security of the cargo and crew.

Compliance with DOT regulation 49 CFR 173.393(j)(4) which deals with radiation levels in occupied vehicles, should be maintained in addition to other applicable State and local requirements. All guards and drivers should be qualified in accordance with AEC Regulatory Guide 5.20, "Training, Equipping, and Qualifying of Guards and Watchman," or an equivalent program.

4. DOOR LOCKS

The cargo compartment doors should normally be in a locked mode and should be secured by a locking mechanism requiring positive action by personnel in both the cargo and cab compartments for operation if the cargo compartment is occupied. If the cargo compartment is not occupied, the cargo compartment door lock should latch closed when shut, and should also be further secured by a padlock. Opening of the cargo compartment door lock should require positive action by personnel at the cargo compartment door and in the cab compartment. The cab compartment doors also should normally be locked and should require key insertion for operation from the outside.

5. ALARM SYSTEM

The vehicle should be equipped with an audible and/or visual alarm which is activated from within the vehicle and which has the same range of detection as that normally required by emergency vehicles. Deactivation of the alarm system circuitry should require access to the armored compartments of the vehicle.

6. SECURING THE CARGO

The vehicle should be supplied with fittings in the cargo compartment to provide an adequate attachment for such securing devices as are required to provide restraint against substantial movement of or damage to the cargo in normal operation and during emergency stops. The cargo must be secured as required by 49 CFR Part 177.

7. RADIATION MEASUREMENTS

Personnel involved in the handling of radioactive material should be provided with a film badge, a pocket dosimeter and for plutonium shipments, a thermoluminescent neutron dosimeter. These should be monitored after each trip.

8. GAS PROTECTION

The vehicle compartments should be equipped with gas masks, filters, or an internal air supply to permit the crew to resist an attack by incapacitating gas for a sufficient time to allow transmittal of a distress message and, if possible, the arrival of aid.

9. ANTENNA PROTECTION

Either a concealed or a hardened antenna should be provided in order to afford sufficient time for the communication system to transmit an emergency message.

10. IMMOBILIZATION

Although there is no requirement for immobilization of vehicles which use armed guards, this is a desirable feature. The vehicle could have a provision for immobilization upon an authorized command originating from within the vehicle. Once commanded, the immobilization system should resist unauthorized deactivation for as long as feasible. Caution should be taken to assure that activation devices which cause immobilization are adequately shielded to prevent them from being energized from spurious electromagnetic signals.

June 1974

U.S. ATOMIC ENERGY COMMISSION

REGULATORY GUIDE

DIRECTORATE OF REGULATORY STANDARDS

REGULATORY GUIDE 5.32

COMMUNICATION WITH TRANSPORT VEHICLES

A. INTRODUCTION

Paragraphs 73.31(b) and 73.33(a) of 10 CFR Part 73, "Physical Protection of Plants and Materials," require that road or rail vehicles transporting special nuclear material in quantities identified in §73.1(b)(2) be equipped with a radiotelephone in order that communication between the transport vehicle and a responsible licensee can be maintained. Paragraph 73.70(g) of 10 CFR Part 73 requires that certain information with regard to the shipment be recorded prior to the shipment. This includes the name of the carriers, major roads to be used, verification of communication equipment on board the transfer vehicle, names of individuals who are to communicate with the transport vehicle, and other information needed to comply with §§73.30 through 73.36 of 10 CFR Part 73. This guide describes radiotelephone equipment and systems, and procedures for their use, that are acceptable to the Regulatory staff for complying with the Commission's regulations regarding radiotelephone communication in connection with road or rail shipments of special nuclear material.

B. DISCUSSION

AVAILABLE SYSTEMS

There are two radiotelephone systems that have a sufficient number of transmitter/receiver stations throughout the country to allow the placement of long distance calls. These are the Bell System Mobile Telephone system and the Radio Common Carrier system (RCC). The Bell system uses three different carrier frequencies [(35, 43), (152, 158), and (454, 459) MHz], and the RCC uses two different carriers [(152, 158) and (454, 459) MHz]. The vehicle receives long distance calls on the lower carrier frequency in each group, i.e., 35, 152, and 454 MHz, and transmits on the higher frequencies, i.e., 43, 158, and 459 MHz. The available channels, which are individual circuits around a particular carrier frequency, for each system are shown in Table I.

TABLE I
NUMBER OF CHANNELS PER CARRIER

	(35, 43) MHz	(152, 158) MHz	(454, 459) MHz
Bell	10	13[a]	12
RCC	None	7	7

[a]11 in U.S., 2 in Canada

The (152, 158) MHz carrier is the most popular throughout the country for both Bell and RCC; the approximate number of cities served by each carrier is shown in Table II.

TABLE II
NUMBER OF CITIES PER CARRIER

	(35, 43) MHz	(152, 158) MHz	(454, 459) MHz
Bell	70	1260	54[a]
RCC	211[b]	625	137

[a]In five of these – Chicago, St. Louis, Dallas, Ft. Worth, and Houston – only local subscribers are served.
[b]Paging service.

USAEC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the AEC Regulatory staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Published guides will be revised periodically, as appropriate, to accommodate comments and to reflect new information or experience.

Copies of published guides may be obtained by request indicating the divisions desired to the U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Director of Regulatory Standards. Comments and suggestions for improvements in these guides are encouraged and should be sent to the Secretary of the Commission, U.S. Atomic Energy Commission, Washington, D.C. 20545, Attention: Chief, Public Proceedings Staff.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust Review
10. General

METHODS OF OBTAINING SERVICE

There are two ways to obtain radiotelephone service. One is to rent the mobile equipment from the Bell System or the Radio Common Carrier (rental will include telephone service and repairs), and the other is to buy the mobile equipment directly from manufacturers and then rent telephone service from either of these systems. Application for equipment rental or telephone service could be made to a local Bell or RCC system company where a licensee or carrier would have most need of the service.

If purchased equipment is to be operated on the Bell System, a license will be required from the Federal Communications Commission (FCC). Purchased equipment operating on the RCC system may not require an FCC license. Maintenance of the equipment is provided when it is leased from the Bell or RCC systems. Purchased equipment must be serviced by licensed operators, as required by FCC regulation 47 CFR 21.207(e), "Transmitter Measurements".

There are several categories which define the priority for obtaining service. These are described in FCC regulation 47 CFR 21.512, "Priorities for service to subscribers."

SYSTEM ASPECTS

There are several types of service and equipment that can be obtained. The service available is dependent on the area. The equipment that can be ordered depends on whether local or nationwide service is desired. In general, the types of service available are:

1. Manual service with access to an operator.

2. Two-way dial with automatic channel selection and access to an operator (also known as Improved Mobile Telephone Service, IMTS).

3. Two-way dial service with access to an operator.

4. Two-way dial service without access to an operator.

The most inclusive service afforded is that of two-way dial with automatic channel selection and access to an operator (IMTS). This service is available on the (152, 158) MHz and (454, 459) MHz carriers only. There are at least two varieties of radiotelephone equipment that can be applied to this service. In one type of radiotelephone operating on the (152, 158) MHz carrier, all eleven channels in the United States are available through the selection of pushbuttons on the telephone. Additionally, three other pushbuttons, Home, Roam, and Manual, are available. When a vehicle is in the Home area the Home pushbutton is depressed and the Home area channels will be selected automatically. When a vehicle is outside the Home area the channels for the particular area must be selected by depressing the channel pushbuttons, as well as the Roam button. The radiotelephone will now automatically select available channels in that area. Another type of radiotelephone operates on the (454, 459) MHz carrier and can automatically select channels in a local area only; it does not have a feature which permits selection of other channels, but could operate in another area on an IMTS mode if the channels were the same as in the Home area.

Other variations in the available equipment are nondialable phones (used only for manual service) and simplex or duplex operation. Simplex operation means that the telephone cannot transmit and receive information simultaneously. That is, while a person talks, he will not be able to hear a response from the other party. To hear the other party, he must stop talking and release a button on the telephone. Duplex operation allows the transmission and receipt of information simultaneously as in normal telephone service.

PREPLANNING

Radiotelephone call-in times can be preplanned in advance of the shipment by using a booklet issued by the American Telephone and Telegraph Co. entitled "National Mobile Telephone Service Area Listing" or a booklet issued by the Radio Common Carrier entitled "Nationwide Service Directory" in conjunction with the route maps to be used with the shipment. The area covered by each base station can be put on the route maps, and radiotelephone call-in times not to exceed 2 hours determined. When a radiotelephone call cannot be planned to occur within a 2-hour period, conventional telephone call-in location and time should be determined. This can initially be determined by locating cities, towns, or populated commercial areas along the route. The conventional call can be preplanned to occur at an approximate time (planned not to exceed 2 hours) from one of these areas. As experience is gained with particular routes, conventional telephone calls can be planned with greater precision. The drivers can note specific telephones or areas where telephones are available along the route for future conventional telephone call-in planning.

COMMUNICATION PROCEDURES

A radiotelephone conversation can be overheard by anyone having a radiotelephone set with the same carrier frequency and channels. It is therefore necessary to disguise the position of the shipment and the routes to be taken. One method for accomplishing this is the use of a transparent nonfoldable grid overlay on a standard road atlas. This grid can consist of one-half-inch squares with the horizontal axis labeled with letters and the vertical axis labeled with numbers. A typical overlay is shown in Figure 1 and is about 10.5 inches by 14 inches in overall dimensions. The road atlas chosen should have a scale of one inch equals 3 miles or less. The resolution of a one-half-inch square on the overlay would then be about 1.5 miles.

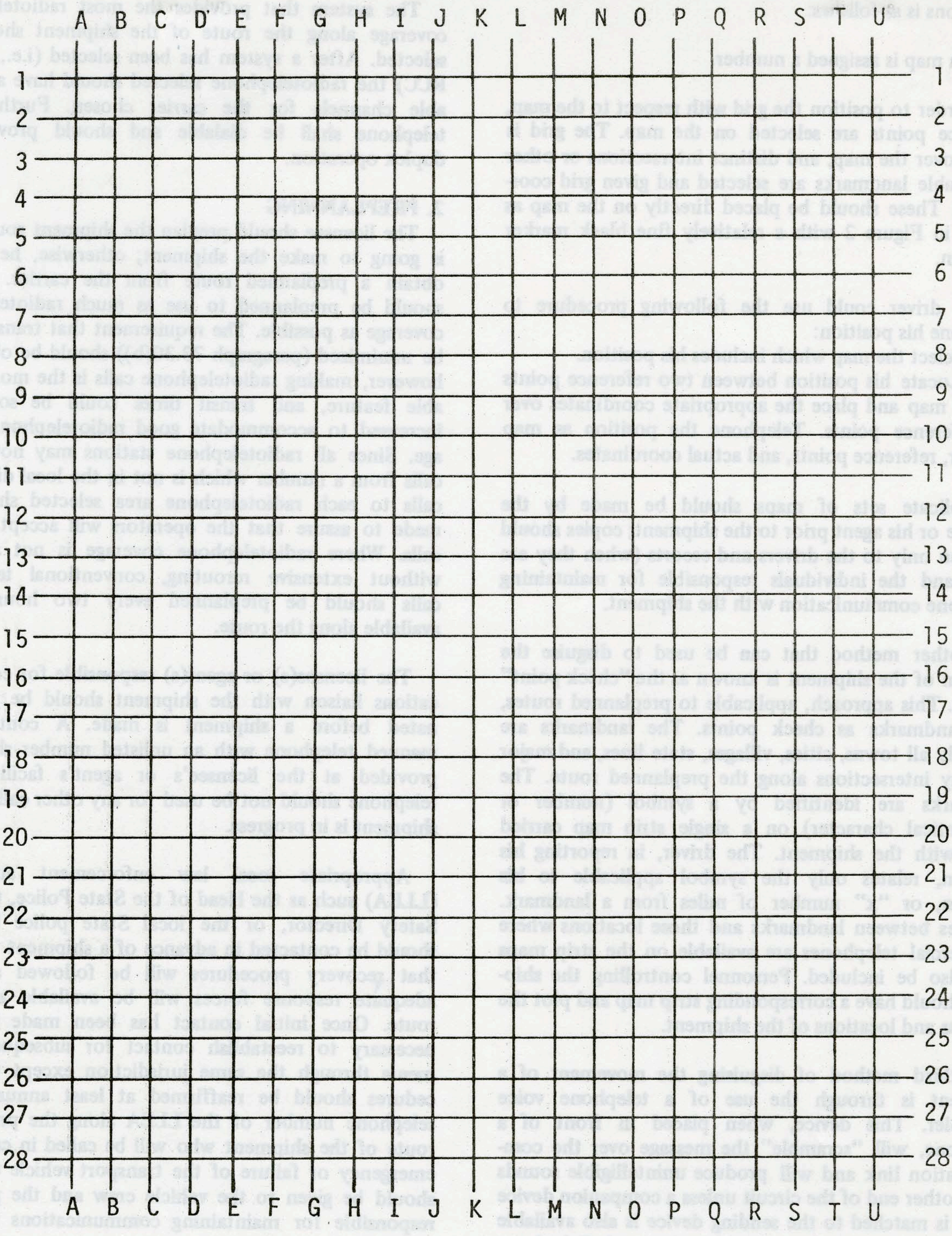


Figure 1. Overlay with 1/2-inch grid (not to scale)

With a scale of one inch equals 3 miles, it may be necessary to use several road maps to cover a shipment. A typical procedure that could be followed under these conditions is as follows:

1. Each map is assigned a number.

2. In order to position the grid with respect to the map, reference points are selected on the map. The grid is placed over the map, and distinct intersections or other identifiable landmarks are selected and given grid coordinates. These should be placed directly on the map as shown in Figure 2 with a relatively fine black marker type pen.

3. The driver could use the following procedure to telephone his position:
   a. Select the map which includes his position.
   b. Locate his position between two reference points on the map and place the appropriate coordinates over the reference points. Telephone the position as map number, reference points, and actual coordinates.

4. Duplicate sets of maps should be made by the licensee or his agent prior to the shipment; copies should be given only to the drivers and escorts (when they are used) and the individuals responsible for maintaining telephone communication with the shipment.

Another method that can be used to disguise the position of the shipment is known as the "check point" system. This approach, applicable to preplanned routes, uses landmarks as check points. The landmarks are typically all towns, cities, villages, state lines, and major highway intersections along the preplanned route. The landmarks are identified by a symbol (number or alphabetical character) on a single strip map carried along with the shipment. The driver, in reporting his position, relates only the symbol applicable to his position, or "x" number of miles from a landmark. Mileages between landmarks and those locations where commercial telephones are available on the strip maps may also be included. Personnel controlling the shipment should have a corresponding strip map and plot the progress and locations of the shipment.

A third method of disguising the movement of a shipment is through the use of a telephone voice scrambler. This device, when placed in front of a telephone, will "scramble" the message over the communication link and will produce unintelligible sounds at the other end of the circuit unless a companion device which is matched to the sending device is also available in front of the telephone at the other end. Telephone voice scramblers are therefore available in coded pairs and can be made available in matched sets of more than two units to handle conference calls or calls from a vehicle to different locations.

C. REGULATORY POSITION

1. SYSTEMS ASPECTS

The system that provides the most radiotelephone coverage along the route of the shipment should be selected. After a system has been selected (i.e., Bell or RCC) the radiotelephone selected should have all available channels for the carrier chosen. Further, the telephone shall be dialable and should provide for duplex operation.

2. PREPLANNING

The licensee should preplan the shipment route if he is going to make the shipment; otherwise, he should obtain a preplanned route from the carrier. Routes should be preplanned to use as much radiotelephone coverage as possible. The requirement that transit times be minimized (paragraph 73.30(b)) should be observed; however, making radiotelephone calls is the more desirable feature, and transit times could be somewhat increased to accommodate good radiotelephone coverage. Since all radiotelephone stations may not accept calls from a number which is not in the local directory, calls to each radiotelephone area selected should be made to assure that the operators will accept outside calls. Where radiotelephone coverage is not available without extensive rerouting, conventional telephone calls should be preplanned every two hours when available along the route.

The licensee(s) or agent(s) responsible for communications liaison with the shipment should be predesignated before a shipment is made. A continuously manned telephone with an unlisted number should be provided at the licensee's or agent's facility. This telephone should not be used for any other calls while a shipment is in progress.

Appropriate local law enforcement authorities (LLEA) such as the Head of the State Police, the State Safety Director, or the local State police barracks, should be contacted in advance of a shipment to assure that recovery procedures will be followed and that adequate response forces will be available along the route. Once initial contact has been made it is not necessary to reestablish contact for subsequent shipments through the same jurisdiction except that procedures should be reaffirmed at least annually. The telephone number of the LLEA along the preplanned route of the shipment who will be called in case of an emergency or failure of the transport vehicle to call in should be given to the vehicle crew and the person(s) responsible for maintaining communications with the vehicle crew.

3. COMMUNICATION PROCEDURES

The check point or voice scrambler is preferred to the grid method for concealing the position of a vehicle. The

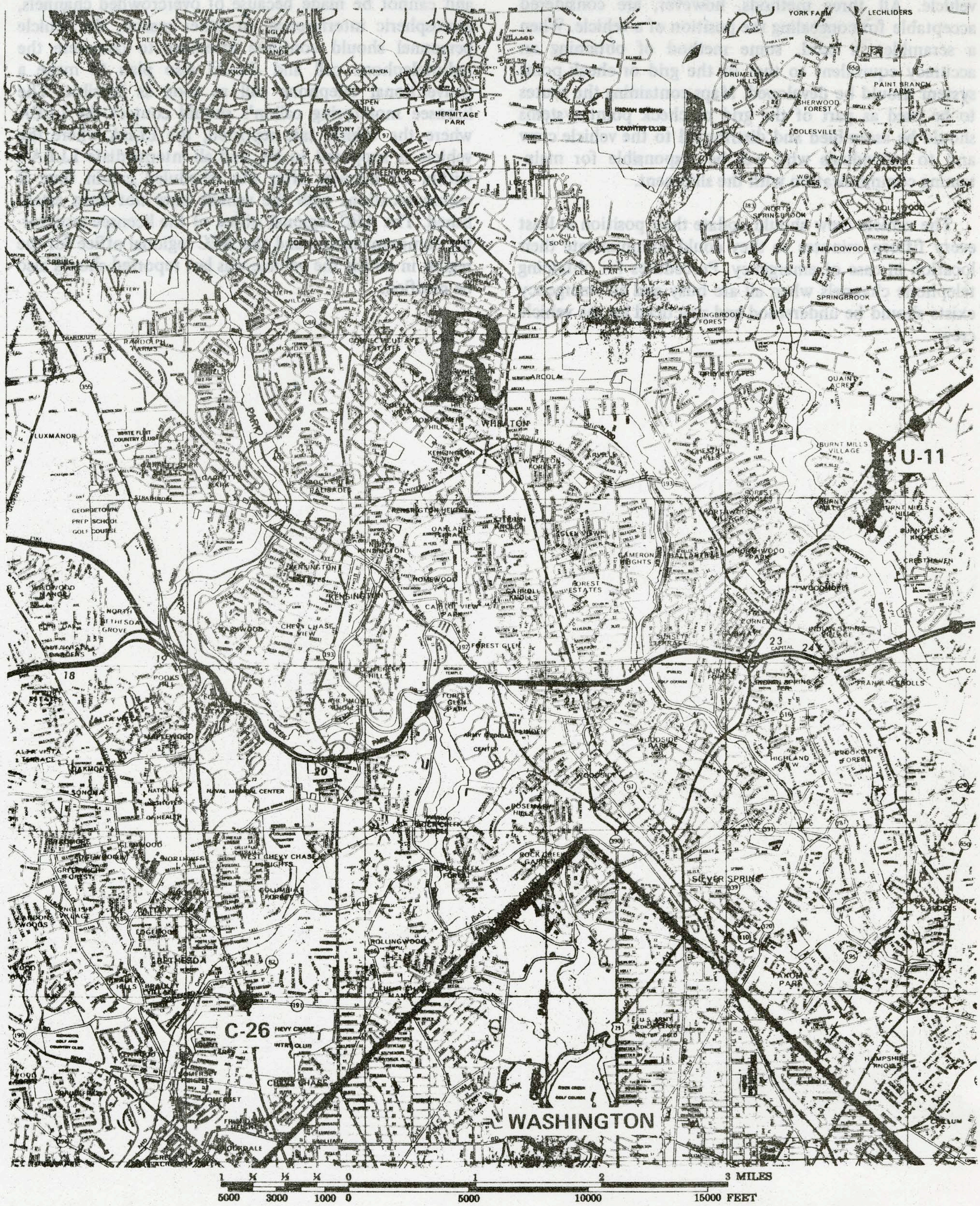


Figure 2. Typical roadmap with grid reference points

grid may offer some operational problem in a moving vehicle. All three methods, however, are considered acceptable for concealing the position of a vehicle. When a scrambler is used, some method of obtaining an accuracy equivalent to that of the grid or check point system should be developed. Maps containing the routes to be used as part of the grid or check point systems should be assembled and distributed to the vehicle crew and to individuals who will be responsible for maintaining communication with the shipment.

The vehicle crew should update their position at least every fifteen minutes so they could communicate their location in case of emergency. Porcedures for obtaining telephone channels when all are busy and an emergency exists should be understood and practiced by the vehicle crew.

In cases where a radiotelephone call has been planned and cannot be made because of overcrowded channels, atmospheric interference, or other reason, the vehicle personnel should continue attempts to complete the radiotelephone call and should also plan to make a conventional telephone call as soon as possible. The licensee monitoring call-in's should contact the LLEA where the vehicle last reported, the LLEA where the vehicle is supposed to be, and all intermediate LLEA's within 30 minutes after the scheduled call-in time if communications with the vehicle have not been established. The AEC regional office of the licensee monitoring communications and the AEC regional office for the region in which the vehicle was last reported should also be notified.

Form AEC-8
(1-67)
AECM 0240

C

INCOMING AND SIGNATURE TAB

Use this side of the sheet to precede the incoming material when assembling correspondence.

(USE REVERSE SIDE FOR SIGNATURE TAB)

16—75922-4 GPO

RECOMMENDATIONS FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL

INTERNATIONAL ATOMIC ENERGY AGENCY

RECOMMENDATIONS FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIAL

Produced
by a panel of experts
working under IAEA sponsorship
in Vienna 6–10 March 1972

Printed by the International Atomic Energy Agency, Vienna, June 1972

CONTENTS

I. INTRODUCTION

1. National safeguards systems have as one of their aims the prevention of diversion of nuclear material. The physical protection of nuclear material is an essential supplement to the State's national system of accounting for and control of nuclear material (hereinafter referred to as the "national system of nuclear materials control").

2. The recommendations for physical protection given in this report have been developed by a panel of experts working under Agency sponsorship. Whilst they are not binding upon States they represent the conclusions of the experts for an optimized system and they are recommended for use by States as required in their physical protection systems.

II. OBJECTIVES

1. The objectives of the States' physical protection system should be:

(a) To establish conditions which will minimize the possibilities for clandestine or overt theft of nuclear material. It should assure the physical protection of nuclear material during storage, use and transit;

(b) To provide for rapid and comprehensive measures by the State to locate and recover nuclear material whether it is stolen, lost, misrouted, late in arrival, etc.

2. The objectives of the Agency are:

(a) To provide a set of recommendations on requirements for the physical protection of nuclear material in storage, use and transit. The recommendations are for consideration by the competent authorities in the States for use in conjunction with their national systems of nuclear materials control. Such recommendations could provide guidance but could not be mandatory upon a State and would not infringe the sovereign rights of States;

(b) To be in a position to give advice to competent national authorities in respect of their physical protection systems at the request of the State. The intensity and the form of assistance required are, however, matters to be agreed upon between the State and the Agency.

III. RESPONSIBILITY

1. The responsibility for the establishment, implementation and maintenance of a physical protection system within a State shall rest entirely with that State.

2. A State may delegate the administration of physical protection measures either to a national body, or to duly authorized persons.

3. The State's physical protection system should be promulgated in co-ordination with the national system of nuclear materials control.

4. In the case of international transfer the responsibility for physical protection measures shall be the subject of agreement between the States concerned.

5. The Agency has no responsibility either for the provision of a physical protection system or for the supervision, control or implementation of such a system. The Agency may informally advise the State of observations made during its normal safeguards activities. Further assistance by the Agency will be provided only when so requested by the State.[1]

[1] INFCIRC/153 paragraph 68 provides that a State shall make special reports without delay to the Agency in the case of possible losses within the State. Similarly INFCIRC/153 paragraph 97 provides for reporting to the Agency in cases of possible losses during international transfers. Corresponding provisions are included in safeguards agreements by the Agency and States other than those which are based upon INFCIRC/153.

IV. COMMON FEATURES OF SYSTEMS FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL IN USE, STORAGE AND TRANSIT

A State's physical protection system should include the following features.

1. Promulgation of Regulations

The State should promulgate and review regularly its comprehensive regulations for the physical protection of nuclear material whether in State or private possession. These regulations should include provision for the timely detection of possible theft of nuclear material.

The State's physical protection system should provide for co-ordination with the State's national system of nuclear materials control.

2. Implementation

Arrangements should be made to ensure that physical protection measures are implemented and that these measures include the following features:

(a) Security survey; (see definition in Annex II)

(b) Licensing after approval of physical protection measures;

(c) Personnel authorization;

(d) Sanctions concerning falsification of nuclear material records and reports;[2] and

(e) Measures to ensure that employees and the public are aware of the danger inherent in the unauthorized removal of nuclear material and to encourage by suitable means their continual co-operation.[2]

The State should confirm that the physical protection requirements are being implemented.

The State should license activities within that State only when they comply with physical protection regulations. It should be noted that other regulations such as those relating to radiological safety may also apply.

The State's physical protection system should make provision for periodic review of the licensed activities to ensure continuous compliance with physical protection regulations.

[2] Although these items are not in themselves physical protection measures, it should be recognized that they could be a valuable part of a State's domestic procedures.

3. Information System

An information system should be provided to notify the State's physical protection system of any changes which may affect implementation.

In addition, the State's physical protection system should have access to information which it requires from the national system of nuclear materials control.

4. Initiation of Recovery System

It is envisaged that despite the existence of preventive measures, a recovery system would also be required.

In circumstances when there is reason to believe that there has been an unauthorized removal of nuclear material, the State's physical protection system should provide for prompt notification to the authority responsible for co-ordination of the State's physical protection activities.

One of the most essential components of an effective system for physical protection of nuclear material is the capability to initiate timely recovery action in case of possible theft or misrouting of the material. This should be done in full co-ordination with the existing public security forces.

Although actual recovery actions may not be part of physical protection measures they must be recognized as an important feature in the development of any domestic procedures. Particular attention must be given whenever international transport of nuclear material is contemplated.

5. Delegation of Authority

The features in 1 through 4 above may be the responsibility of one single authority, or they may be divided amongst separate competent authorities provided that arrangements are made for overall co-ordination.

A State may delegate the administration of physical protection measures either to a national body, or to duly authorized persons. It is implicit in such cases of delegation that the State satisfies itself that the physical protection arrangements conform to the requirements laid down by the State. Furthermore, the duly authorized persons shall be fully responsible for the continuing confirmation of complete compliance with the physical protection measures.

V. GENERAL REQUIREMENTS FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL IN USE AND STORAGE

1. Protected Area

Nuclear material in Groups I and II (see Annex I) should be used or stored only within a protected area (see Annex II).

2. Movements of Nuclear Material

Movements of nuclear material within a protected area are the responsibility of the operator and he should apply all prudent and necessary physical protection measures.

Movements out of or between two protected areas are to be treated in full compliance with the requirements for nuclear material in transit after taking account of prevailing conditions.

3. Access

Access to nuclear material within a protected area should be restricted and closely controlled.

4. Control of Nuclear Material

Arrangements should be made in any protected area to avoid the possibility of unauthorized nuclear or substitute material being carried into or out of the area.

5. Process Sub-Stores

Nuclear material in mid-process or in process substorage must be deemed to be in storage at all times when the facility is not in normal operation, e.g. overnight when under single shift operation, at week-ends or during holidays. Protection measures appropriate to storage should be applied at those times.

VI. DETAILED REQUIREMENTS FOR PHYSICAL PROTECTION OF NUCLEAR MATERIAL IN USE AND STORAGE

1. General Statement

This section has been designed to identify, so far as possible, the elements comprising an effective physical protection system for Groups I and II material in use and storage. Considerable flexibility has been incorporated into the element descriptions and optimal features have been described. Special attention should be given to the situation where the sum of the quantities of nuclear material held in adjacent or contiguous buildings is sufficient to enter a protection category or to pass from Group II to Group I.

2. Essential Features for Groups I and II Material

The essential features for Groups I and II material should be:

(a) Protected Area (see definition in Annex II): nuclear material should be used or stored only in a protected area.

(b) Security Survey (see definition in Annex II): a security survey should be made at least annually (or whenever a significant change in the facility, or its function takes place) by the State's physical protection authority to evaluate the effectiveness of the physical protection measures, and to identify necessary changes in measures so as to optimize their effectiveness in particular situations at the facility.

Furthermore, plant operators should maintain checks on the efficient functioning of the physical protection measures.

(c) Facilities which handle, use or store nuclear material should be so arranged that the number of entries and exits is minimized (ideally only one). All emergency exits should be fitted with alarms (see definition in Annex II) if specified by the security survey. Any ground level windows should be permanently locked where possible, or covered with firmly embedded bars. Facilities should not be sited close to public thoroughfares, if possible.

In the case of Group I material there should be a readily available communication capability to local police or other public security forces.

For Groups I and II material the access of all persons and vehicles entering or exiting the area should be checked. This includes checking packages, loads, etc. Special consideration should be given to the advisability of preventing the entry of private motor vehicles inside protected areas.

(d) Admittance Controls (see definition in Annex II) should be used at all points of entry to protected areas and within them to storage areas or other buildings or rooms when these contain nuclear material of Group I or II. All persons entering the protected area should be issued either special passes or badges, appropriately registered. These should follow the general outline below:

Type I: Employees whose duties permit or require continual access to areas containing nuclear material, including nuclear material records keepers and members of the management. Issue of passes or badges should be limited to those authorized by the State's physical protection authority.

Type II: Other regular employees; these should be determined by facility normal practices.

Type III: Temporary repair, service or construction workmen; these should be escorted by a Type I badged employee at all times when they may have access to nuclear material.

Type IV: Visitors; these should be escorted by any badged employee at all times in the protected area and by a Type I badged employee when they may have access to nuclear material.

Passes and badges should be designed so as to make counterfeiting extremely difficult.

(e) All employees should be frequently (about annually) informed of the importance of effective physical protection measures and trained in their implementation. Notices on the subject should be conspicuously posted throughout the facility.

(f) Nuclear material handlers should be required to conform to procedures for transferring custody of the nuclear material to the succeeding handler.

Additionally, nuclear material handlers should endeavour to ascertain on reporting for duty that no interference or theft has taken place and to report to a senior authority whenever they have reason to believe that a discrepancy may exist.

(g) A record should be kept of all persons having access to or possession of keys concerned with the containment or storage of nuclear material. Arrangements should be made for:

- the checking of keys, particularly to minimize the possibility of duplication; and
- the changing of combinations at suitable intervals.

Locks should be changed when compromised.

(h) Emergency plans of action should be prepared to effectively counter any possible threats to nuclear material, including attempted diversion, accident or natural disaster. Such plans should provide for the training of facility personnel in their actions in case of alarm or emergency.

In addition, personnel trained by the facility should be prepared to meet all necessary demands of physical protection and recovery and should act in full co-ordination with external emergency forces and safety response teams, who should also be appropriately trained.

3. Additional Essential Features for Group I Material

The essential features for Group I material, additional to those in 2 above should be:

(a) The perimeter of the protected areas should normally consist of a physical barrier (see definition in Annex II) in addition to and outside of the building walls. However, where the walls of a building are of such solid construction as to be designated, as a result of a security survey, as being the perimeter of a protected area, they should be supplemented by a surveillance system outside the building walls.

(b) A 24 hour guarding service should be provided. The guard (see definition in Annex II) should report at scheduled intervals to local police or other public security forces during non-working hours.

(c) An external and internal patrol (see definition in Annex II) should be provided.

(d) In all cases where separate storage structures are used they should be of the "strong room" type in design and must be located within a protected area. They should be provided with adequate locks and the issue of keys should be closely controlled. Access to storage must be strictly limited to assigned officials and to others only when under their escort. Where nuclear material is stored overnight in work areas, or in a sub-storage structure within a work area, specially authorized procedures should be used to protect the area. Alarms, patrols, or TV monitors would satisfy this requirement.

4. Additional Essential Features for Group II Material

The essential features for Group II material, additional to those in 2 above should include either:

(a) a separate guarded physical barrier fitted with alarms; or

(b) external and internal building alarms.

In either case, where alarms are used, they should be so connected as to initiate reaction by public or private security personnel within the shortest possible time.

5. Optional Features for Groups I and II Material

(a) Alarms of various types which give an appropriate response to indicate forced entry or unauthorized presence may be used to assist guards as required.

(b) Tamper indicating seals may be used in conjunction with locks or on infrequently used containers holding nuclear material. Such seals should be serialized and otherwise resistant to counterfeiting and their integrity should be checked daily.

(c) TV monitors may be used as required to minimize manned surveillance (see definition in Annex II) in certain areas containing nuclear material or at other parts of the facility. They may be used together with alarms and may record observations for later examination. These recordings should be checked hourly or the screen should be constantly watched by personnel.

(d) Doorway monitors designed to detect uranium and plutonium may be used.

VII. GENERAL REQUIREMENTS FOR NUCLEAR MATERIAL IN TRANSIT

1. Hazards

A State's physical protection system should be designed to cover, so far as practicable, the following types of hazard in transit:

- improper routing;
- damage;
- accidents;
- hijacking;
- theft;
- sabotage;
- interference; or
- substitution en route.

The existence of these hazards increases the relative danger of the transit situation as compared with use and storage.

2. Division of Measures

The measures required may conveniently be divided into those to be taken in advance, those to be applied between despatch and receipt and those to be applied after receipt. The following recommendations are accordingly made for the protection of nuclear material in transit.

3. Measures prior to Shipment of Groups I and II Material

3.1. Advance Notification to Receiver

The readiness of the receiver to accept delivery at the expected time of arrival should be ascertained prior to the commencement of the shipment.

3.2. Advance Notification to Other Bodies

In cases where advance notifications have to be despatched to various bodies by virtue of safeguards obligations and radiological safety regulations, it is suggested that such notifications be made use of whenever they might be regarded as useful for purposes of physical protection, provided that the necessary cross-links exist between the appropriate bodies.

3.3. Advance Authorization

In cases covered by adequate regulations, routine shipments may be carried out without the obligation to seek case-by-case authorization or to notify the national control authority in each particular case in advance.

In all cases not covered by existing regulations or going beyond boundary conditions defined in such regulations, consent of a national control authority to a transport operation should be sought in advance. This implies the performance of an appropriate security survey in advance. Furthermore, the transport permission may include specific limitations and conditions related to the particular circumstances and to whatever emergency plans have been prepared.

3.4. Marking and Coding

It is undesirable to advertise transport operations if this could lead to a decrease in the degree of physical protection. This requires great restraint in the use of any special markings, inspections on vehicles, etc., and in particular on the use of open channels for the transmission of messages concerning shipments of nuclear material. When such messages are required by safeguards or radiological safety regulations, consideration should be given to the extent practicable, to measures such as coding and appropriate routing; care should be exercised in the handling of such information. These considerations also apply to any subsequent communications.

3.5. Selection of Transportation and Routing

In choosing the route, consideration should be given to the security of passage. The transport method for any given consignment should be such as to keep to a reasonable minimum the number of cargo transfers and the length of time the cargo remains in the transport means. The co-operations of the carrier concerning the implementation of physical protection measures should be ensured in advance.

4. Measures in Actual Transit

Greater variations may be expected in the implementation of measures for the physical protection of nuclear material in transit than in the case of nuclear material in storage or use where a greater measure of uniformity can be recommended.

The general measures to be adopted during the actual transportation of nuclear material of Group I are given below:

(a) monitoring/escorting/guarding;

(b) emergency response capability; and

(c) communication.

In the case of Group II material some, but not all the measures are essential.

The extent to which these measures will be used by persons actually accompanying the consignment or respectively stationed centrally, or at various points along the route of the consignment will depend upon the particular conditions prevailing in the State. It should, however, be ensured that these functions are properly exercised and integrated into a viable and reliable system.

VIII. DETAILED REQUIREMENTS FOR NUCLEAR MATERIAL IN TRANSIT

1. Different Needs in Each State

This section was prepared in full recognition that nuclear material in transit is in an environment vulnerable to theft and which does not lend itself readily to conventional techniques for physical protection. It is recognized that the different structures of the nuclear industry, transportation services and geography in different States make it impossible to find a single structure for transportation safeguards that will provide for uniform effectiveness and be uniformly practicable. Accordingly this document identifies certain basic requirements applicable to all nuclear material transportation and then provides for alternatives from which each State may design its own system in such a manner as to achieve the desired goals.

2. Aims

It has been recognized that two basic aims must be achieved to reduce the vulnerability to theft during transportation. These are:

(a) minimize the total time during which nuclear material remains in the transportation environment; and

(b) minimize the number of transfers of the nuclear material during transportation, i.e. transfer from one vehicle to another, transfer to temporary storage awaiting transportation vehicle arrival, etc.

3. Methods

To achieve these basic aims, several possibilities are suggested, these are:

(a) Use a single dedicated vehicle or aircraft exclusively for each nuclear material shipment (i.e. full load concept) and despatch it on a non-stop schedule using seals wherever possible.

(b) Use air transport, cargo aircraft where possible.

(c) Despatch escorts (see definition in Annex II) or guards with each shipment who should expedite its handling, particularly at transfer points. Such escorts or guards should be effective in avoiding misrouting which among other dangers prolongs the time the material remains in transit. They may also be used to manage problems related to safety during accidents.

(d) Use monitors to meet the transportation vehicle at each scheduled transfer point to avoid misrouting described in (c) above.

(e) Ensure that the intended receiver will check the integrity of the packages and seals, and accept the shipment immediately upon arrival. The packages should not be left in a vehicle until the next working day.

4. Communication and Emergency Action

Conventional physical protection measures are not operative in transportation in the same way or with the same preventive results as in the environs of a facility. Although audible alarms, for example, may be used in both environments, the transportation vehicle may be in a remote area, out of hearing range for a response action. This example demonstrates a key need for effective transportation safeguards, communication and response. Ideally, vehicles carrying nuclear material should be constantly monitored by the communication system and arrangements should be made to provide an adequately sized and trained response force.

The latter should reach the scene of a theft from transportation either while it is in process so they can prevent its successful completion or immediately after its completion so they can optimize the possibility of recovery. Domestic transportation safeguards should include frequent or continuous communication with vehicles carrying nuclear material and should include a programme to establish teams who would be trained to react and provide assistance in emergency or delay. Such teams would be sited at strategic locations within the State.

5. Routing

Vehicles carrying nuclear material should be routed in such a way as to avoid areas of troubles (either human or natural). In addition, the State's physical protection system should minimize the danger that may arise when vehicle operators leave their vehicle for any reason, including refreshment stops or the like. In some cases two-man operation may be required and may be essential for Group I material.

6. Essential Requirements

The following list contains the essential requirements for a State's transportation system, except that items marked* are optional for Group II material.

(a) Advance communication with the receiver to assure his readiness to accept delivery.

(b) Pre-routing of transport vehicle to avoid troubled or violent areas.

(c) Arrangements to ensure that minimum journey time and transfers are involved.

(d) Telephone or telegraph communication between shipper and receiver at expected arrival time to achieve prompt recognition of possible diversion.

(e) Arrangements with the carrier to ensure that vehicle operators will not leave the vehicle unattended at any time during transit.

*(f) Optimized communication with the shipment en route by one of the following means:
(i) constant radio;
(ii) checkpoint reports from designated observers en route; or
(iii) scheduled phone reports from the vehicle operator.

(g) Optimized arrangements for the despatch of trained teams to prevent successful completion of a theft in process or to initiate efforts to recover diverted material. The teams should be designated by a State from its military units, public security organizations, specially designated units or combinations thereof.

*(h) Development, and use when developed, of mechanisms to thwart or delay thieves, such as:
(i) vehicle disabling system when under recognizable threat from diverters;
(ii) cargo tie down or lacking systems to delay removal of nuclear material;
(iii) alarm mechanisms, e.g. emission of coloured smoke to enhance locating vehicle under threat, particularly in remote areas.

(j) Advance planning of temporary storage of nuclear material during transport. Access to the temporary storage should be limited.

7. Additional Considerations

In addition to the essential elements in 6 above, for Group I material, States should consider the need to insist upon the use of guards or escorts to accompany the shipment of monitors at transfer points to insure proper handling of the cargo at all transfers. These measures should be used where conditions indicate a need for such services, particularly where several transfers are necessarily involved.

All problems connected with the domestic transport of nuclear material also arise in connection with international transport. However, some of them become more complex in the international context. Additional problems also arise.

8. Necessity for Advance Agreements

In the case of international transport between two States sharing a common frontier the State's responsibility for physical protection and the point at which physical protection responsibilities transfer from one State to another should be the subject of an agreement between the States. However, with respect to the maintenance of communication regarding the continuing integrity of the shipment and with respect to the responsibility for carrying out a maximum recovery effort in the event that a shipment becomes lost, the agreement between the States should provide that this responsibility will rest with the shipping State up to the frontier and then will transfer to the receiving State.

When international shipments transit the territory of States other than the sending State and the recipient State, the arrangements between the

shipping and receiving States should, to the extent practicable, identify the States involved in such transit with a view to securing in advance their co-operation and assistance for recovery actions on the territory of such States in case of loss of an international shipment thereon.

States may wish to consider the possibility of establishing a convention wherein States could aid each other in the recovery of nuclear material in any cases where such aid would be of value.

ANNEX I

GROUPING OF NUCLEAR MATERIAL FOR PHYSICAL PROTECTION

In developing a physical protection system a State should take account of:

(a) the accessibility of material for diversion, which depends on physical form, isotopic and chemical composition, etc;

(b) the quantity of nuclear material involved;

(c) the location of the material, i.e. in use, storage or transit; or

(d) the particular circumstances prevailing either in the State or along the transportation route.

The following Table gives the two groupings of the different types of nuclear material taking into account quantities and isotopic composition. These groupings have been used throughout the contents of this document.

Material	Group I	Group II
U-233, Pu, U enriched to 20% U-235 or more, or mixtures thereof	More than 5 ekg	More than 1 ekg
U enriched to 5% U-235 or more and less than 20% U-235	-	More than 5 ekg
U at enrichments above natural, but less than 5% U-235	-	10 t

Note:

(a) ekg is defined in INFCIRC/153 as follows: "effective kilogram" means a special unit used in safeguarding nuclear material. The quantity in "effective kilograms" is obtained by taking:

(i) for plutonium, its weight in kilograms;

(ii) for uranium with an enrichment of 0.01 (1%) and above, its weight in kilograms multiplied by the square of its enrichment;

(iii) for uranium with an enrichment below 0.01 (1%) and above 0.005 (0.5%), its weight in kilograms multiplied by 0.0001; and

(iv) for depleted uranium with an enrichment of 0.005 (0.5%) or below, and for thorium, its weight in kilograms multiplied by 0.00005.

(b) For the purposes of physical protection the following are cases which may not enter Group I or II even though the quantities of nuclear material involved put them into either Group I or II:

(i) irradiated fuel because it requires heavy shielding, special handling equipment and expensive chemical reprocessing; and

(ii) material which is not easily handled for other reasons, e.g. batches comprising large drums of waste.

(c) The exclusion of certain small quantities of nuclear material from the group definitions should not be interpreted to mean that they should not be protected. It is expected that such material be protected through prudent management practices.

ANNEX II

DEFINITIONS

1. Admittance Control

A system providing for limiting by appropriate checks the entrance or exit to the passage of identifiably authorized persons and material.

2. Alarm

A technical device for the purpose of sensing intrusion or interference. Such a device should be independent of any power supply failure. It should be arranged to signal any interference with its function.

3. Door Monitors

A passive device for the purpose of detecting the passage of nuclear material.

4. Guard or Escort

A person entrusted with surveillance or access control, his duties should be specified by the security survey.

5. Patrol

A person or persons (who may be guards) scheduled to inspect barriers, seals or other features at regular or irregular intervals.

6. Physical Barrier

A physical barrier is a fence or wall or a similar impediment approved by a security survey.

7. Protected Area

A protected area is an area under constant surveillance (by a guard for Group I material; by a guard or by electronic means for Group II material surrounded by physical barrier and having a limited number of controlled admittance points and approved by a security survey.

8. Security Survey

A critical examination made by competent officers, in order to evaluate, approve and specify physical protection measures.

9. Surveillance

Close observation to be achieved by invigilator (personnel), photo electric, closed circuit television, sonic detectors, electronic, photographic, or other means.

ANNEX III

PANEL ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL
VIENNA 6 - 10 MARCH 1972

List of Participants, Observers and Agency Staff Members

I. Participants	Home Address
M. Billy	Commissariat à l'énergie atomique, 29-33 rue de la Fédération, Paris XV, France
L. Brenner	USAEC, Division of Nuclear Materials Security, Washington, DC 20545, United States of America
G.J. Dorogov	State Committee on Utilization of Atomic Energy, Staromonetny Preulok 26, Moscow, USSR
D. Gupta	Institut für Angewandte Reaktorphysik, Postfach 3640, 75 Karlsruhe 1, Federal Republic of Germany
H. Kurihara	Atomic Energy Bureau Science and Technology Agency, Policy Division (Agency staff member since 30 May 1972) Tokyo, Japan
O. Lendvai	National Atomic Energy Commission, P.O. Box 565, Budapest V, Hungary
A.E. Ross	UKAEA, Reactor Group, Risley, Warrington, Lancs, United Kingdom
N. Srinivasan	Bhabha Atomic Research Centre, Fuel Reprocessing Division, Bombay, India

II. Observers

S. Abiko	Power Reactor and Nuclear Fuel Development Corporation, Nuclear Fuel Division, 1-9-13 Akasaka, Minato-ku, Tokyo, Japan
S. Hagsgaard	AB Atomenergi, Studsvik, 611 01 Nyköping, Sweden
G.L. Hanna	Permanent Mission of Australia to the IAEA, Concordiaplatz 2/III, 1010 Vienna, Austria (Australia)
K. Heil	Bundesministerium für Bildung und Wissenschaft, Heussallee 2 - 10, 53 Bonn 9, Federal Republic of Germany
A. Nedelik	Österreichische Studiengesellschaft für Atomenergie, Seibersdorf, Austria
A. Pilgenröther	Nukem GmbH, Wolfgang bei Hanau, Federal Republic of Germany
R.E. Tharp	USAEC, Washington, DC 20545, United States of America
L.W. Thorne	British Nuclear Fuels Ltd, Risley, Warrington, Lancs, (Agency staff member since 4 April 1972) United Kingdom

III. Agency Staff Members

E. López-Menchero	Director, Division of Development
B.C. Bernardo G.E. Swindell	Division of Nuclear Safety and Environmental Protection
P. Ha-Vinh	Legal Division
R.A. Borthwick M. Ryzhov	Division of Development
D.F. Rawson	Scientific Secretary, Division of Development

Form AEC-8
(1-67)
AECM 0240

INCOMING AND SIGNATURE TAB

Use this side of the sheet to precede the incoming material when assembling correspondence.

(USE REVERSE SIDE FOR SIGNATURE TAB)

16—75922-4 GPO

D

APPENDIX D

PROJECTED IMPROVEMENTS IN CURRENT U.S. STANDARDS

Following the enactment of legislative authority in August of this year:

1. Requirements are being established for prior government trustworthiness determinations for all individuals who will have access to sabotage-vulnerable areas of nuclear power industrial facilities or who will have access to or custody of radioactive materials in quantities and types that could be used for nuclear explosive fabrication or as radioactive contamination weapons.

2. Studies are currently being conducted to determine

   a. Ways to improve armed guard protection for facilities and materials including the question of whether such services should be provided by government personnel as opposed to private corporate individuals.

   b. Grouping and siting of fuel cycle plants to reduce and possibly eliminate transportation of potential target materials.

   c. Designs for transportation vehicles which will provide considerable hardening against attempts to sabotage or hijack shipments.

   d. The practicability of using massive shipping containers to make the removal of potential target materials from transport vehicles more difficult for potential saboteurs and thieves.

   e. Mechanisms for providing constant communication with transportation vehicles and escort vehicles while enroute and for providing automatic location of such vehicles to enhance reaction efforts in the event of an alarm.

f. Ways in which physical barriers, currently required by regulations, can be strenthened.

g. Penalty modes that would be triggered by illicit attempts to breach access control mechanisms. These penalty modes would be designed to provide further time delay for the accomplishment of the illicit act. Such things as debilitating gases, smoke, etc., are being considered.

h. The possible application of advanced access control systems such as fingerprint identification, etc.

i. Ways in which the radiological properties of special nuclear material might be changed to inhibit the use of such material in the manufacture of an illicit nuclear explosive device.

In addition, certain other changes are ready to be implemented. These are:

1. A minimum of two armed guards must escort all shipments (ground, air and seas) of the specified quantity and type of special nuclear material (see 10CFR 73)
2. Constant communication with transport vehicles carrying the special quantity and type of SNM.
3. Implementation and publicizing of safeguards rewards.
4. Requirement to use "hardened" vehicles for transport.
5. A study geared to the strengthening of the physical barriers for fixed sites.

Form AEC-8
(1-67)
AECM 0240

INCOMING AND SIGNATURE TAB

Use this side of the sheet to precede the incoming material when assembling correspondence.

(USE REVERSE SIDE FOR SIGNATURE TAB)

16—75922-4 GPO

E

APPENDIX E

6/18/74

IAEA SAFEGUARDS & THE NPT

To understand the Non-Proliferation Treaty it is essential to understand the role, status, and effectiveness of the safeguards system which is to police the non-proliferation guarantees given by the parties to the Treaty. If the degree of validity and meaning of these safeguards is not accurately understood, our premise for relying on and supporting the Treaty is weakened. The continued effectiveness of safeguards is the factor most likely to have bearing on the long-term preservation and stability of the Treaty. It is probably safe to say that if IAEA safeguards had been applied to the CIR Reactor in India, the May 18 explosion would not have occurred.

1. Introduction

A major issue impeding final agreement on the language of the NPT was the question of whether and how the Treaty could be policed. Article III, on safeguards, was the last Article to be written and agreed. There was an option, which the U.S. rejected, that there should be no policing; that the word of sovereign nations would provide sufficient assurances that the parties were honoring their non-proliferation undertaking; (backed up by national intelligence gathering organizations which, hopefully, would give a warning if a party was violating that undertaking). Article III was finally agreed, calling for the IAEA to apply its safeguards to police the Treaty undertaking.

An important question to consider in appraising the value of the NPT is the status and meaningfulness of those safeguards, to the extent that it can be determined at this early date in the life of the Treaty; What assurances will the system give? (And what can't it give?) How technically valid are the assurances? Will the assurances be sufficiently meaningful and valid to warrant our reliance on them? What technical, political, and organizational problems does the system have? What might be done to upgrade the effectiveness of the system?

2. Brief Technical Description of IAEA Safeguards

Objective

The objective of applying IAEA safeguards to nuclear materials in facilities is: (a) the timely detection of government instigated (or supported) diversion of significant quantities of that material from peaceful nuclear activities; and (b) the deterrence of such diversion through the risk of early detection and sanctions. To detect diversion, the IAEA must verify the quantities and location of safeguarded nuclear material.

6/18/74

Sanctions

If the Agency finds, in applying safeguards in a given situation, there has been a diversion or that it is not able to verify that there has been no diversion, and after giving the subject country reasonable opportunity to furnish sufficient explanation and reassurances, the Agency will report the non-compliance to its Board of Governors, all members of the Agency and the Security Council and General Assembly of the United Nations. The Agency may also suspend rights and privileges of Agency membership, curtail or suspend assistance and call for the return of materials and equipment which may have been provided.

Elements of the System

Nuclear materials accountancy is the fundamental IAEA safeguards tool with containment and surveillance as important complementary measures. Accountancy is essential to knowledge of how much safeguarded material is supposed to be at a facility and, therefore, determination of how much may have been diverted. To permit good accountability, facilities have to be designed to permit adequate measurement and control of the nuclear materials being processed or used in them. The IAEA reviews nuclear facility design from this point of view. Detailed and accurate records and periodic reports need to be kept and submitted to keep track of the inventories, input, process losses, wastes, and shipments of nuclear materials. The IAEA reviews the system of records and reports for adequacy. The Agency also processes the periodic reports to assist in planning inspections, follow the flows of materials and check for quantity agreement between shippers and receivers. This data also can be evaluated to determine if significant uncertainties are developing in the measurement of nuclear material quantities flowing through a process. The Agency conducts periodic inspections to audit and verify information in records and reports, to account for the material by independent measurement, to review the methods of measurement, to investigate process losses and sources of uncertainties in the inventory and throughput, and to read and service containment and surveillance devices. Containment and surveillance techniques (such as tamper indicating seals on stored nuclear materials, or tamper resistant automatic cameras providing unmanned observation of nuclear material in storage) give evidence whether there may have been unreported changes in the quantities of nuclear material in a given location since the last inspection.

Technical Conclusions

The technical conclusions of the Agency's verification activities are statements, covering defined areas in which safeguarded nuclear material has been stored, used or processed, of the amounts of nuclear material unaccounted for over a specific period, giving the limits of accuracy of the amounts stated. If the amounts which cannot be accounted for are significant and cannot be reasonably explained, the political procedures noted in the "sanction" section above may be initiated.

3. Role of IAEA Safeguards

IAEA safeguards play a role in two general areas: (a) to police the NPT undertakings of non-nuclear weapons states (N-NWS') party to the Treaty; and (b) to police undertakings of non-NPT parties with respect to individual facilities and shipments of nuclear material, which undertakings the countries have given to suppliers as a condition of supply or have given unilaterally to the Agency.

NPT Safeguards Agreements

The IAEA's safeguards under NPT agreements are applied on all source or special fissionable material in all peaceful nuclear activities in the N-NWS party to the Treaty, with a view to preventing diversion of nuclear energy from peaceful uses to nuclear weapons or other nuclear explosive devices. Thirty such agreements were in force at the end of March 1974, although only 17 of the countries had nuclear programs requiring safeguards implementation.

Non-NPT Safeguards Agreements

Under non-NPT agreements, IAEA safeguards are applied to select nuclear activities in the non-NPT party country with a view toward ensuring that the special fissionable or other materials, services, equipment facilities, and information under Agency controls are not used in such a way as to further any military purpose. Forty-one such agreements are in force dealing with specific facilities in 23 non-NPT countries, plus the U.S. and the U.K. Examples are the two U.S.-supplied power reactors at Tarapur, India; the two Canadian-supplied power reactors at Rajasthan, India; the Research Reactor at Nahal Soreq, Israel; the major fraction of the Japanese and Swiss nuclear programs, research reactors in Argentina, South Africa, Brazil, etc. The U.S. interprets its NPT obligations as permitting cooperation with and supply to activities in non-NPT countries if IAEA safeguards apply to the U.S. assistance and if it is clearly understood by the recipient country that the U.S. considers "peaceful nuclear explosives" to be prohibited by the recipients undertaking not to further any military purpose.

Effect of Safeguards

The desired effect of IAEA safeguards is: (a) to deter national level diversion of safeguarded nuclear material by the governments of the countries involved; (b) to place a responsibility on those governments to institute domestic programs which would deter sub-national level diversion of safeguarded nuclear material (i.e., by individuals or groups acting contrary to Government policy); (c) to reduce specific international

OFFICIAL USE ONLY

tensions by providing a degree of assurance among countries, especially hostile neighbors, that the safeguarded country is not developing nuclear weapons; and (d) more generally, create an environment of confidence that, to the extent safeguards are being applied, international nuclear commerce to exploit the peaceful benefits of nuclear energy can be freely conducted without contributing to insecurity and tension among nations.

Range of Effectiveness

It would be difficult if not impossible to prove whether or to what degree the safeguards actually accomplish the desired effects, as described above. Although certain technical conclusions can be derived from safeguards activities, the overall extent to which the safeguards are effective, as applied, is largely a matter of speculation/judgment. However, there is clearly a broad range of technical and procedural rigor possible in the implementation of the safeguards system which would bear on the effectiveness; from occasional visits to facilities involving minimal independent verification activities (basically "window dressing") to a tight, statistically based, highly independent technical program of verification. If the final judgment is that, regardless of the rigor of the system, the assurances will not be sufficient, then there is no need to pursue the more rigorous (and more costly) approach. In any event, it is important to have in mind where on the scale we want the system to be, and to what extent we are getting what we want.

4. Important Things IAEA Safeguards Do NOT Do

It is important to recognize the limitations of IAEA safeguards. Several key limitations are identified below:

(a) IAEA safeguards under NPT agreements do not preclude a country from using nuclear materials in military programs as long as those programs are not developing nuclear weapons or other nuclear explosive devices, (e.g., naval propulsion programs are permitted). Further, if a country wishes to use nuclear material in such a non-proscribed military use, Agency safeguards will not be applied to that material and no international controls to verify non-diversion to nuclear weapons or other nuclear explosive devices would be in effect for those activities. If an outside supplier wants to prevent his assistance from being used in this way under NPT safeguards agreements, he must enter into a special understanding to this effect with the IAEA and the recipient country, as the U.S. has done.

(b) IAEA safeguards under non-NPT agreements are specifically against "furthering any military purpose." Several countries consider this to allow development of peaceful nuclear explosives. Therefore, the U.S., U.K., Canada, and some other suppliers have made general public statements and specific private statements to recipients of assistance that we consider the peaceful use

OFFICIAL USE ONLY

guarantees to preclude the use of safeguarded material for any nuclear explosive device; and that IAEA safeguards, even under non-NPT safeguards agreements, are to check this.

(c) IAEA safeguards under NPT agreements cover only <u>declared</u> peaceful nuclear activities; both indigenously supported activities, and those supported by outside suppliers. The IAEA has no authority nor ability to seek out undeclared or clandestine activities. Under non-NPT safeguards agreements, the IAEA might apply safeguards at only one minor facility out of a large civil nuclear program involving many facilities. The IAEA would have no authority with respect to those other facilities unless safeguarded nuclear material was transferred to them.

(d) IAEA safeguards measures are limited to accountancy, passive containment, and surveillance. The Agency has no authority to implement physical protection measures (against nations) in safeguarded activities, such as armed guards, locks and other exclusion devices, pursuit and capture of diverted material, etc. These measures can only be employed by sovereign nations (against subnational groups or individuals) which have legal bases and jurisdiction for applying the force inherent in them. Therefore, IAEA safeguards provide no physical protection against overt takeover of safeguarded nuclear material for military purposes, but rather only an assurance that such takeover would be discovered and reported.

(e) IAEA safeguards are not foolproof; the system cannot provide absolute assurances that nuclear material has not been diverted. In situations where large quantities of nuclear material are being used or processed, technical limits on the ability to measure inventories and throughput of nuclear material will leave large uncertainties in the actual quantities being safeguarded. If the safeguarded country or facility operator has more sophisticated and accurate control of his nuclear material than the IAEA is aware of and can detect, diversion within the limits of IAEA uncertainty might take place without detection. It is a question of competition for technological competence.

5. <u>Current Problem Areas in IAEA Safeguards System</u>

There are several areas in which the evolving IAEA safeguards program is encountering difficulties. Many of these problems are being actively worked on by Agency personnel and by groups in some of the interested IAEA member countries and it is expected (hoped) that the problems can be solved.

The underlying general problem is that of transforming an idea (that an international group can be formed with responsibility to devise and implement a technically sound plan which will verify that sovereign nations are not diverting nuclear material) into a practical and effective reality. There are no precedents to look at in solving this problem. More specifically, there are three problem areas; political/financial, technical/procedural, and organizational.

Political/Financial Problems

Safeguards cost money* and good safeguards cost a lot of money. The U.S., USSR, Canada, and a few other smaller countries have been active promoters and supporters of the NPT and its safeguards. The remaining IAEA member nations, including those party to the Treaty, have either been generally passive, or openly negative regarding these safeguards. With such a low level of political support, there is a corresponding low level of enthusiasm for financial support. This became evident when the group of 50 nations which drew up the structure and content of NPT safeguards agreements in 1971 required that a special formula be developed for apportioning the cost of Agency safeguards among the IAEA membership. Under this formula, the cost, which is paid out of the Agency's regular budget, is borne in a slightly higher proportion by the more developed countries, than the cost of the remaining IAEA operations. Additional stark evidence was given this past April when several members of the IAEA Board of Governors complained that IAEA safeguards costs were too high in relation to IAEA expenditures for technical assistance to the less developed countries. Proposals were made that IAEA safeguards manpower should be frozen at the 1974 levels and that less developed countries should not have to pay more toward the safeguards portion of the budget then they paid in 1971 (this latter was an Indian suggestion). Many nations have expressed the view that IAEA safeguards primarily benefit the major powers (U.S., U.K., USSR) and, therefore, the major powers should pay for the safeguards. Without more widespread political support for IAEA safeguards it will be difficult to raise sufficient funds to conduct an effective safeguards program.

* The IAEA's safeguards budget for 1975 is 5 million dollars out of a total Agency budget of 26.5 million.

OFFICIAL USE ONLY

6/18/74

Technical/Procedural Problems

A. Develop sophisticated nuclear materials measurement techniques, preferably non-destructive and unmanned, which allow Agency inspectors to verify quantities of all nuclear materials which have gone through a safeguarded process or which are in storage in a safeguarded nuclear facility. Sometimes these materials are not directly accessible for physical sampling (e.g., they might be contained in a $50,000 fuel assembly which would have to be destroyed to put the nuclear material in a form which could be measured; or they might be in a highly radioactive solution in a tank behind six feet of concrete. The inspector's problem is to try to verify, with as much certainty as the facility operator can verify it, how much nuclear material is in that assembly or tank). The Agency must keep in the forefront of nuclear material measurement techniques. Industry must be able to accept the reasonableness of these techniques. For example, where a proprietary process is used, can the inspector employ methods of verification which do not require access to the process?

B. Develop independent procedures and techniques to apply these quantity verification measures to inventories and flows of nuclear material using limited rights of access (duration and location) within safeguarded facilities and with limited dollar and manpower resources; i.e., optimize cost-effectiveness of techniques and procedures.

C. Develop more effective containment and surveillance techniques. As larger facilities and flows of nuclear material are encountered, nuclear material accountancy becomes a less powerful deterrent to a possible significant diversion and the assurances gained by accountancy must be supplemented by containment and surveillance techniques to assure that the material which cannot be accounted for is not leaving the plant undetected.

D. Assure to the extent possible that the procedures and techniques are non-intrusive and do not impede the safe, economical operations of the facility.

E. Develop computer programs to organize, process, and evaluate the very large amounts of data which will be submitted in reports to the Agency and brought in as a result of inspections.

F. Assure that all the separate facets of measurement techniques, inspection procedures, containment and surveillance, data handling and processing, etc., fit into a logical, balanced, effective, coherent system which meets the desired objective.

G. Determine the most practical way of using the domestic safeguards systems of governments in nations where IAEA safeguards are applied, recognizing the difference in their objectives, techniques, and authority, and maintaining the necessary independence of the Agency's verification activities. Determine how this can be done in detailed practice in the special case of Euratom and its multi-national safeguards system.

H. Determine how to relate and evaluate the technical conclusions of safeguards implementation (e.g., the quantity of nuclear material that cannot be accounted for) from several individual safeguards areas (e.g., several nuclear facilities) in order to arrive at a rational and meaningful conclusion about whether or not the country involved is in non-compliance with the NPT. Set up the process by which it would be officially decided that a diversion is suspected or has taken place; the procedures to follow in case a diversion is suspected.

I. Determine and be prepared for the possible impact of possible future nuclear technology on the efficacy and meaning of safeguards - e.g., simple isotope separation techniques, widespread use of highly-enriched uranium and plutonium in HTGRs and breeder reactors, fusion power, etc.

Organizational Problems

A. Determine optimum organizational structure to develop and carry out the IAEA's safeguards obligations. Is the current structure the best?

B. Most effective ulitization of manpower, when initial assignments are for two years and when there has to be a balance of nations represented on the staff without full regard for availability of talent.

C. Logistics problems involving international travel for inspections; moving instruments, visas and ease of passage from country to country (e.g., to investigate special incidents involving possible loss or diversion of nuclear materials), regional offices vs. a central office in Vienna, international shipping and handling of radioactive samples taken by inspectors, etc.

D. Problems associated with language and cultural differences (e.g., the impediment to effectiveness when a non-oriental is trying to inspect a facility where the routine communications and records are in Japanese; or, trying to hire, for safeguards, a Japanese-speaking individual with a good background in nuclear technology who is not a Japanese national owing political allegiance to Japan).

E. Develop effective safeguards inspector training techniques.

6. Possibilities of Strengthening Agency Safeguards

The following suggestions would need further detailed elaboration and evaluation before being considered for adoption:

6/18/74

A. Educational efforts to increase political support by other countries - stressing the benefits to them of the NPT and of effective IAEA safeguards.

B. Press for higher level of safeguards financing; look for new possibilities of financing.

C. Increase level of U.S. unilateral and cooperative support for current problem areas through, e.g., U.S. R&D efforts, making available expert consultants, competent U.S. nationals on IAEA safeguards staff, IAEA safeguards training and procedure exercises at U.S. facilities, etc.

D. Within the existing IAEA safeguards guidelines (INFCIRC/153 and INFCIRC/66/Rev. 2) press for full implementation making maximum use of the rights already provided to obtain independent verification.

E. Upgrade the IAEA safeguards guidelines (INFCIRC/153 and INFCIRC/66/Rev. 2) to provide for greater access and independence of IAEA inspectors (e.g., such as originally granted in the IAEA Statute).

F. Upgrade IAEA's safeguards authority, e.g., more flexible and wider range of sanctions, powers in the physical security field, greater international mobility, regional offices, laboratories and staffs with necessary diplomatic immunities.

G. Upgrade and increase IAEA role in setting standards (and possibly checking for compliance with them) in National systems of safeguards, especially in the area of physical security.

H. Establish a high-level, highly competent Safeguards Review Committee to critically monitor IAEA safeguards development and implementation and suggest areas where improvement in effectiveness and efficiency are needed.

(Following are more far reaching and radical possibilities to consider:

I. Modify the IAEA Statute and/or the NPT to provide stronger IAEA safeguards responsibility and authority.

J. Transfer the safeguards responsibility from the IAEA to a separate, independent organization, possibly loosely affiliated with the IAEA or, more directly, with the UN.)

7. <u>NPT Article III.2. and the Nuclear Exporters Group (Zangger Committee)</u>

Article III.2. of the NPT calls for states to refrain from providing nuclear material or equipment especially designed or prepared for the processing, use, or production of nuclear material to any non-nuclear weapons state for peaceful purposes, unless the nuclear material shall be subject to IAEA safeguards. Seventeen major nuclear supplier nations (excluding France) have voluntarily formed an ad-hoc group in order to work out a common minimum interpretation of this provision, so as to minimize the likelihood of safeguards requirements influencing international commercial competition. The group has developed minimal guidelines which have not yet been made publicly known, although it is hoped to make them public in the near future. The impediment to moving ahead is the fact of French non-cooperation and the resulting possibility that France would freely supply the critical material and equipment, thus undermining the objectives of the group and the NPT, and at the same time making sales which others have denied themselves the opportunity to make. The objective of this effort is to deny the ten or so relatively capable (technically) countries which are non-signatories to the NPT from an external source of safeguards-free nuclear materials and equipment. The guidelines do not cover supply of nuclear technology inasmuch as this is not covered by NPT Article III. However, they do provide a clear understanding that, although the safeguards to be applied are not pursuant to NPT safeguards agreements, they would be aimed at diversion to nuclear weapons or other nuclear explosive devices.

Successful efforts to increase the scope of coverage over materials and equipment and to enlist further members for the group have the effect of spreading the application of safeguards. Without a corresponding increase in financial and political support for IAEA safeguards the probable effect would be to decrease the effectiveness of those safeguards.

JFMahy/plg
SS/USAEC
6/18/74