Collection: Counterterrorism and Narcotics, Office of, NSC: Records
Folder Title: VPTF (Vice President's Task Force) Recommendations/Status Reports March 1987 Ted McNamara/NSC Staff (2)
Box: RAC Box 10

WITHDRAWAL SHEET
Ronald Reagan Library

Collection: COUNTERTERRORISM AND NARCOTICS, NSC: Records

Archivist: dlb

File Folder: VPTF (Vice President's Task Force) Recommendations/ Status Reports March 1987 Ted McNamara/NSC Staff (2) ~~Box 91956~~ PAC

Date: 11/1/00 Wills/F97-082/2

DOCUMENT NO. AND TYPE	SUBJECT/TITLE BOX 10	DATE	RESTRICTION
1. Addendum	Confidential Addendum to a Report to Congress on Passenger Vessel and Port Security, 9 p. D 3/27/06 NLSF97-082/2 #4	2/87	P1/F1
2. Memo	Philip Haseltine to Rodney McDaniel, re: Final Status Report on Implementation of NSDD 207, 5 p.	5/20/86	P1/F1

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]
- P-1 National security classified information [(a)(1) of the PRA].
- P-2 Relating to appointment to Federal office [(a)(2) of the PRA].
- P-3 Release would violate a Federal statute [(a)(3) of the PRA].
- P-4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA].
- P-5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA].
- P-6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA].

C. Closed in accordance with restrictions contained in donor's deed of gift.

Freedom of Information Act - [5 U.S.C. 552(b)]
- B-1 National security classified information [(b)(1) of the FOIA].
- B-2 Release could disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA].
- B-3 Release would violate a Federal statue [(b)(3) of the FOIA].
- B-4 Release would disclose trade secrets or confidential commercial or financial information [(b)(4) of the FOIA].
- B-6 Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA].
- B-7 Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA].
- B-8 Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA].
- B-9 Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA].

ANNEX 1

SECURITY SURVEYS

1 General

1.1 In order to prepare security plans, an initial comprehensive security survey should be undertaken to assess the effectiveness of security measures and procedures for the prevention of unlawful acts and determine the vulnerability of the port facility or the ship, or both, to such acts.

1.2 The results of this security survey should be used to determine the security measures necessary to counter the threat both at the port facility and on board ships taking into consideration local conditions.

1.3 The level of security may vary from port to port, from ship to ship and from time to time. Liaison between security officers is important to ensure the best utilization of ship and shore resources.

1.4 The survey should determine what needs to be protected, what security measures are already in effect, and what additional security measures and procedures are required.

1.5 The security survey should be periodically reviewed and the security plans updated as necessary.

2 Port facility security survey

2.1 The port facility security survey may be divided into two parts, the initial preliminary assessment and an on-scene security survey.

2.1.1 Preliminary assessment

2.1.1.1 Prior to commencing the survey the port facility security officer should obtain current information on the assessment of threat for the locality and should be knowledgeable about the port facility and type of ships calling at the port. He should study previous reports on similar security needs and know the general layout and nature of the operations conducted.

2.1.1.2 The port facility security officer should meet with appropriate representatives of the port facility, of the operator, or of both of them, to discuss the purpose and methodology of the survey.

2.1.1.3 The port facility security officer should obtain and record the information required to conduct a vulnerability assessment, including:

.1 the general layout of the port facility and terminal including topography, building locations, etc.;

.2 areas and structures in the vicinity of the port facility such as, fuel storage depots, bridges, locks, etc.;

.3 the degree of dependence on essential services, such as electric power, communications, etc.;

.4 stand-by equipment to assure continuity of essential services;

.5 locations and functions of each actual or potential access point;

.6 numerical strength, reliability and function of staff, permanent labour and casual labour forces;

.7 the details of existing security measures and procedures, including inspection, control and monitoring procedures, identification documents, access control procedures, fencing, lighting, fire hazards, storm drains, etc.;

.8 the equipment in use for protection of passengers, crews and port facility personnel;

.9 all vehicle traffic or services which enter the port facility; and

.10 availability of other personnel in an emergency.

2.1.2 On-scene security survey

2.1.2.1 The port facility security officer should examine and evaluate the methods and procedures used to control access to ships and restricted areas in the port facility, including:

.1 inspection, control and monitoring of persons and carry-on articles;

.2 inspection, control and monitoring of cargo, ship stores, and baggage; and

.3 safeguarding cargo, ship stores and baggage held in storage within the port facility.

2.1.2.2 The port facility security officer should examine each identified point of access to ships and restricted areas in the port facility and evaluate its potential for use by individuals who might be engaged in unlawful acts. This includes persons having legitimate access as well as those who seek to obtain unauthorized entry.

2.1.2.3 The port facility security officer should examine and evaluate existing security measures, procedures and operations under both emergency and routine conditions, including:

.1 established safety procedures;

.2 restrictions or limitations on vehicle access to the port facility;

.3 access of fire and emergency vehicles to restricted areas and availability of parking and marshalling areas;

.4 the level of supervision of personnel;

.5 the frequency and effectiveness of patrols by security personnel;

.6 the security key control system;

.7 security communications, systems and procedures; and

.8 security barriers and lighting.

3 Ship security survey

3.1 The ship security survey may be divided into two parts, the initial preliminary assessment and an on-scene security survey.

3.1.1 Preliminary assessment

3.1.1.1 Prior to commencing the ship security survey, the operator security officer should take advantage of such information as is available to him on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their security measures. He should study previous reports on similar security needs.

3.1.1.2 Where feasible, the operator security officer should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the survey.

3.1.1.3 The operator security officer should obtain and record the information required to conduct a vulnerability assessment, including:

.1 the general layout of the ship;

.2 the location of areas which should have restricted access, such as bridge, engine-room, radio-room etc.;

.3 the location and function of each actual or potential access point to the ship;

.4 the open deck arrangement including the height of the deck above the water;

.5 the emergency and stand-by equipment available to maintain essential services;

.6 numerical strength, reliability and security duties of the ship's crew;

.7 existing security and safety equipment for protection of passengers and crew; and

.8 existing security measures and procedures in effect, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

3.1.2 On-scene security survey

3.1.2.1 The operator security officer should examine and evaluate the methods and procedures used to control access to ships, including:

.1 inspection, control and monitoring of persons and carry-on articles; and

.2 inspection, control and monitoring of cargo, ship's stores and baggage.

3.1.2.2 The operator security officer should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might be engaged in unlawful acts. This includes individuals having legitimate access as well as those who seek to obtain unauthorized entry.

3.1.2.3 The operator security officer should examine and evaluate existing security measures, procedures and operations, under both emergency and routine conditions, including:

.1 established security procedures;

.2 response procedures to fire or other emergency conditions;

.3 the level of supervision of the ship's crew, vendors, repair technicians, dock workers, etc.;

.4 the frequency and effectiveness of security patrols;

.5 the security key control system;

.6 security communications systems and procedures; and

.7 security doors, barriers and lighting;

4 Periodic security inspections

Security inspections should be undertaken on a periodic basis to permit a review and updating of the initial comprehensive security survey and possible modification of the port facility and ship security plans.

5 Report

5.1 From the information obtained during the survey assessment and inspection, the respective security officer should assess the vulnerability of the port facility, ship, or both.

5.2 The report should contain, as appropriate, recommendations for new or revised security measures and procedures.

5.3 The report will form the basis for development or revision of security plans, should be confidential and have limited distribution.

* * *

ANNEX 2

SECURITY MEASURES AND PROCEDURES

1 General

1.1 Port facility security measures and procedures and ship security measures and procedures should take account of the recommendations contained in the report described in paragraph 5 of annex 1.

2 Port facility security

2.1 Security measures and procedures reduce port facility vulnerability. Increased levels of threat will have a significant influence on the number and type of security measures used and the degree of measures and procedures adopted. During short periods of heightened threat, increased security can be achieved through the use of additional manpower.

2.2 The following on-scene security measures should be considered:

.1 restricted areas;

.2 security barriers;

.3 security lighting;

.4 security alarms and communication systems; and

.5 access control and identification.

2.2.1 Restricted areas

The establishment of restricted areas helps control and channel access, improves security and increases efficiency by providing degrees of security compatible with the port facility's operational requirements. Restricted areas may be further subdivided depending on the degree of restriction or control required to prevent unauthorized access.

2.2.2 Security barriers

2.2.2.1 The boundary between restricted and uncontrolled areas should be clearly defined. This can be achieved by security barriers which prevent access except at authorized points. Where permanent security barriers are appropriate, security fences have proven effective.

2.2.2.2 The purpose of security barriers is to:

.1 delineate the area to be protected;

.2 create a physical and psychological deterrent to persons attempting unauthorized entry;

.3 delay intrusion, enabling operating personnel and security guards to detect, and, if necessary, apprehend intruders; and

.4 provide designated and readily identifiable places for entry of personnel and vehicles into areas where access is restricted.

2.2.2.3 Openings in security barriers should be kept to a minimum and secured when not in use.

2.2.2.4 Security fences and other barriers should be located and constructed so as to prevent the introduction of dangerous substances or devices, and should be of sufficient height and durability to deter unauthorized passage.

2.2.2.5 Security fence lines should be kept clear of all obstructions.

2.2.2.6 The effectiveness of a security fence against penetration depends to a large extent on the contruction employed. The total height of the security fencing should be not less than 2.50 metres.

2.2.2.7 Natural barriers such as water, ravines, etc., can sometimes be effectively utilized as part of the control boundary. However, they may require supporting safeguards (i.e. fencing, security patrols, surveillance, anti-intrusion devices, lighting) especially during high threat periods.

2.2.2.8 The roofs of buildings may also provide a possible route for unauthorized access to the restricted area. Safeguards should be taken to prevent such access by these routes.

2.2.2.9 Restricted areas partly surrounded by water may require security barriers with sufficient illumination during night hours and, if on navigable waters, frequent and unscheduled patrols by boat or ashore on foot, or both. Illumination of these areas must be of a type and so placed that it does not interfere with safe navigation.

2.2.3 Security lighting

2.2.3.1 Security lighting with uninterrupted power supply is an important element in a security programme.

2.2.3.2 The primary system should consist of a series of lights arranged to illuminate a specific area continuously during the hours of darkness or restricted visibility. In some circumstances, it may be preferable to use such lighting systems only in response to an alarm.

2.2.3.3 Floodlights may be used to supplement the primary system and may be either portable or fixed. Floodlights when used should have sufficient flexibility to permit examination of the barrier under observation and adjacent unlighted areas.

2.2.3.4 Multiple circuits may be used to advantage in the security lighting system. Circuits should be so arranged that the failure of any one lamp will not affect a series of others.

2.2.3.5 Controls and switches for security lighting should be protected at all times.

2.2.3.6 Where fences and other barriers are to be illuminated, it is important to ensure that the intensity of illumination is adequate for the purpose.

2.2.4 Security alarms and communication systems

2.2.4.1 Intrusion detection systems and alarm devices may be appropriate as a complement to guards and patrols during periods of increased threat.

2.2.4.2 Immediate response capability by guards to an alarm from an intrusion detection system or device is important if its use is to be effective. Alarms may be local, i.e. at the site of the intrusion, provided at a central location or station, or a combination of both.

2.2.4.3 A wide variety of intrusion detection systems and devices are available for possible use. These systems include those which are sensitive to:

.1 breaking of an electrical circuit;

.2 interruption of a light beam;

.3 sound;

.4 vibration;

.5 motion; or

.6 capacitance change in an electrical field.

2.2.4.4 In view of the wide range of technical matters which must be taken into account in deciding upon the device or system best suited for application in each environment and for each task, it is prudent to obtain the advice of a qualified expert before a decision is made on the system or device to be used.

2.2.4.5 A means of transmitting discreet or covert signals by radio, direct-line facilities or other similarly reliable means should be provided at each access point for use by the control and monitoring personnel to contact police, security control, or an emergency operations centre in the event assistance is required. An additional public or overt communications system would be useful to obtain information or advice on routine matters.

2.2.5 Access control and identification

2.2.5.1 Persons and their property, before being permitted to proceed beyond access points, should be subject to routine inspection or control and monitoring, or both.

2.2.5.2 It is recommended that port facility employees, vendors, operators' personnel, assigned law enforcement officials and others, whose official duties require them to pass through the access point, should prominently display a tamper-resistant identification card. This procedure should be closely monitored and strictly enforced to preserve the integrity of the inspection, control and monitoring processes and the security of the passenger terminal and ships. Approved means of identification and the procedures to be followed should be specifically provided for in the security plan.

2.2.5.3 An effective means of identification is a card which incorporates a photograph of the individual as an integral part. These should show the relevant details of the holder, e.g. name, description, or other pertinent data. The provision of a photograph is recommended in order to prevent misuse of the card by unauthorized persons.

2.2.5.4 To prevent substitution of a photograph and subsequent illegal use, the entire card should be sealed in a plastic container, preferably of a type which will mutilate the photograph and card if tampered with.

2.2.5.5 The number and types of different styles of identification cards in the port area should be limited in order to avoid control problems for security staff and the administration of the identification programme.

2.2.5.6 Identification cards should be issued by an appropriate control authority, such as a port authority or ship operator. Strict card control and accountability procedures should be established and maintained.

2.2.5.7 Persons who refuse to submit to security clearance at an access point must be denied entry.

2.2.5.8 Persons denied entry for refusal to submit to security clearance, or for other security reason should be, if possible, identified and reported to appropriate security personnel.

2.2.5.9 A booth or other area in which a manual search can be conducted is advisable. The access points should, as appropriate, be equipped with metal detectors to expedite the security clearance of people.

2.2.5.10 All items should be subject to inspection, appropriate to the risk of unlawful acts, prior to being placed on board ships. Such inspection methods may include hand search, electronic screening, the use of dogs, or other means.

2.2.5.11 Tables on which baggage may be searched should be provided at the appropriate access points. Such tables should be high enough to permit inspection without requiring the examiner to bend. They also should be sufficiently wide to provide some measure of separation of the baggage from the passenger. The latter should be able to witness the examination, but should not be in a position to interfere with the examiner.

3 Ship security

3.1 The master's traditional authority in matters of ship security remains unchanged. Maintaining ship security is an ongoing task. Additional security measures should be implemented to counter increased risks when warranted.

3.2 Ship security should be continually supervised by the ship security officer. A properly trained crew is in itself a strong deterrent to being subjected to unlawful acts.

3.3 Communication and co-operation with the port facility in security matters should be maintained.

3.4 The following on-board security measures should be considered:

.1 restricted areas;
.2 deck and overside lighting;
.3 access control and identification; and
.4 security alarms and communication systems.

3.4.1 Restricted areas

3.4.1.1 The establishment of restricted areas on board ships (e.g. bridge, engine-room, radio-room etc.) is recommended.

3.4.1.2 The use, number and distribution of master keys on-board ships should be controlled by the master.

3.4.1.3 The ship security plan should provide for immediate corrective action in the event of security being compromised by potential misuse or loss of keys.

3.4.2 Deck and overside lighting

3.4.2.1 While in port, at anchor or underway the ship's deck and overside should be illuminated in periods of darkness and restricted visibility, but not so as to interfere with the required navigation lights and safe navigation.

3.4.3 Access control and identification

3.4.3.1 Crew members should carry at all times a photo identification document.

3.4.3.2 When visitors to the ship are permitted their embarkation and disembarkation should be closely controlled.

3.4.3.3 All vendors should have an identification document prior to boarding the ship or should be escorted at all times on board the ship.

3.4.4. Security alarms and communication systems

3.4.4.1 Security alarms and devices may be appropriate in restricted areas and at access points to the ship, as a complement to guards and patrols. Immediate appropriate response to an alarm is important if the security alarms and devices are to be effective.

3.4.4.2 In view of the wide range of technical matters which must be taken into account in deciding upon the device or system best suited for application in each environment, it is prudent that the advice of a qualified expert be obtained before a decision is made on the system or device to be used.

3.4.4.3 A means of discreet or covert communications by radio, direct-line facilities or other reliable means should be provided in each restricted zone and at each access point for use by security or operating personnel to contact the ship security officer in the event assistance is required.

* * *

ANNEX 3

SECURITY TRAINING

1 General

A continuous and thorough training programme should support measures taken to safeguard the security of passengers and crews on board ships. Basic guidance for development of security training and education is given in the following paragraphs.

2 Criteria

Security training should meet the following criteria:

.1 be comprehensive;
.2 have an adequate number of qualified instructors;
.3 have an effective system of presentation;
.4 use adequate training equipment and aids; and
.5 have a clearly defined objective, i.e. the attainment of an established minimum standard of proficiency, knowledge and skill to be demonstrated by each individual.

3 Port facility security personnel training

3.1 Security officer and appropriate staff

The port facility security officer and appropriate port facility staff should have knowledge and, as necessary, receive training in some or all of the following, as appropriate:

.1 security administration;
.2 relevant international conventions, codes and recommendations;
.3 responsibilities and functions of other involved organizations;
.4 relevant government legislation and regulations;
.5 risk, threat and vulnerability assessments;
.6 security surveys and inspections;
.7 ship security measures;
.8 security training and education;
.9 recognition of characteristics and behavioural patterns of persons who are likely to commit unlawful acts;
.10 inspection, control and monitoring techniques;
.11 techniques used to circumvent security measures;
.12 dangerous substances and devices and how to recognize them;
.13 ship and local port operations and conditions; and
.14 security devices and systems.

3.2 Inspection, control and monitoring

Instruction and, where appropriate, training for persons assigned to conduct inspection, control and monitoring at a port facility should take into consideration, as appropriate:

.1 responsibilities under the port facility plan or ship security plan;
.2 inspection, control and monitoring regulations or policies and pertinent laws;
.3 detection and identification of fire-arms, weapons and other dangerous substances and devices;

.4 operation and testing of security equipment;

.5 manual search methods of persons, baggage, cargo and ship's stores;

.6 emergency procedures;

.7 recognition of characteristics and behavioural patterns of persons who are likely to commit unlawful acts;

.8 human relations techniques; and

.9 techniques used to circumvent security measures.

3.3 Guards

Port facility guards who are assigned either to specific fixed locations or to patrols for the purpose of preventing unauthorized access to areas should receive a general briefing on the training subjects recommended for the port facility security officer. Initial and subsequent training should emphasize techniques for:

.1 entry control;

.2 patrols, observation and communications;

.3 inspection, identification and reporting;

.4 person, building and vehicle searches;

.5 apprehension of suspects;

.6 self-defence;

.7 recognizing dangerous substances and devices;

.8 human relations; and

.9 first aid.

4 Ship security personnel training

4.1 Operator security officer and appropriate staff

The operator security officer and appropriate staff should have knowledge and, as necessary, receive training in some or all of the following, as appropriate:

.1 security administration;
.2 relevant international conventions, codes and recommendations;
.3 responsibilities and functions of other involved organizations;
.4 relevant government legislation and regulations;
.5 risk, threat and vulnerability assessments;
.6 security surveys and inspections;
.7 ship security measures;
.8 security training and education;
.9 recognition of characteristics and behavioural patterns of persons who are likely to commit unlawful acts;
.10 inspection, control and monitoring techniques;
.11 techniques used to circumvent security measures;
.12 dangerous substances and devices and how to recognize them;
.13 ship and local port operations and conditions; and
.14 security devices and systems.

4.2 Ship security officer

The ship security officer should have adequate knowledge of and, if necessary, training in the following, as appropriate:

.1 the ship security plan and related emergency procedures;
.2 the layout of the ship;
.3 the assessment of the risk, threat and vulnerability;

.4 methods of conducting security inspections;

.5 techniques used to circumvent security measures;

.6 operation of technical aids to security, if used;

.7 recognition of characteristics and behavioural patterns of persons who may be likely to commit unlawful acts;

.8 the detection and recognition of dangerous substances and devices;

.9 port and ship operations; and

.10 methods of physical searches of persons and their baggage.

4.3 Inspection, control and monitoring personnel

Instruction and training, as appropriate, for persons assigned to conduct inspection, control and monitoring on board ships should take into consideration, as appropriate, the following:

.1 responsibilities under the port facility or ship security plan;

.2 inspection, control and monitoring regulations or policies and pertinent laws;

.3 detection and identification of fire-arms, weapons and other dangerous substances and devices;

.4 operation and testing of security equipment, if used;

.5 physical search methods of persons, baggage, cargo and ship's stores;

.6 emergency procedures;

.7 recognition of characteristics and behavioural patterns of persons who are likely to commit unlawful acts;

.8 human relations techniques; and

.9 techniques used to circumvent security measures.

4.4 Ship's crew

Crew members having specific security duties should know their responsibilities for ship security as described in the ship security plan and should have sufficient knowledge and ability to perform their assigned duties.

5 Law enforcement personnel

Appropriate law enforcement personnel, when not directly involved in or responsible for port facility security, should receive a general briefing to become familiar with port and ship operations and the training of port facility and ship operator security personnel. They should also be orientated regarding inspection, control and monitoring and the security plans.

* * *

ANNEX 4

EXCHANGE OF INFORMATION

1 The prompt and continuing dissemination and exchange of information will assist the maintenance of effective port and ship security procedures and will enable States, port facilities, operators and shipmasters to adjust their procedures in response to changing conditions and the specific or general threats.

2 Effective port and ship security requires efficient two-way communications for the exchange of information at all levels both domestic and with the governments and organizations concerned. The prompt, clear and orderly dissemination of such information is vital to the success of the security programme.

***

APPENDIX 2

PORT VULNERABILITY ASSESSMENT

To determine facility vulnerability, 10 major factors are considered. They are as follows:

--Port Facility Characteristics

--Type of Security Force

--Physical Security Measures

--Routes of Access/Egress

--Communications

--Availability of Additional Port Security Resources

--Response Time/Distance for Security Personnel

--Time/Contiguousness to Urban Areas

--Local Social Environment

--Proximity to International Borders

The "Quantification Factors" follow: (Point Values are not to be Interpolated)

1. Port Passenger Terminal Facility Characteristics and Sensitivity (14 points).

_____ Mission Sensitivity.

Dedicated Passenger Terminal:	3 Points
Military Port Facility (Naval Base or MOT):	3 Points
Commercial Port Facility:	2 Points
POL Facility:	1 Point

NOTE: Select best port description

_____ Current Threat Analysis.

Unavailable:	3 Points
Available:	0 Points

Quantification Factors (cont'd)

_____ Port Accessability.

Port Facility, Uncontrolled Access, No Gate Guard or Patrol Force 2 Points

Port Facility, Uncontrolled Access, No Gate Guard but Patrol Force 1 Point

Port Facility, Controlled Access, Gate Guard but no Patrol Force 1 Point

Port Facility, Controlled Access, Gate Guard and Patrol Force: 0 Points

_____ Port Volume Capacity. (measured in tons per year moved if cargo port) (Passenger ports are measured in passengers per year moved)

CARGO PORT

High (Over 25 million tons) 2 points.

Medium (10 million to 25 million tons) 1 point.

Low (Under 10 million tons) 0 points.

PASSENGER PORTS

High (Over 10,000 passengers): 2 Points

Medium (1000-10,000 passengers): 1 Point

Low (Under 1000 passengers): 0 Points

NOTE: When port is utilized for both use highest vulnerability.

_____ DOD Assets within the Port Facility.

Yes: 1 Point

No: 0 Points

_____ SIV access.

Available: 3 Points

Unavailable: 0 Points

2. Port Security Force: (12 Points).

COMMENTS: Consideration should be given to the type of guard force utilized, whether contract guard force or state port police; variations in training requirements; local "use of force" policy.

_____ No Security Guard Force or Trained Port Facility Security Personnel: 12 Points.

_____ Port Security Manager, No Security Guard Force or Trained Port Facility Security Personnel: 9 Points.

_____ Port Security Manager, Security Guard Force or Port Facility Security Personnel in Place but Poorly or Not Trained: 6 Points.

_____ Port Security Manager, Trained Port Security Personnel, Not Fully Equipped: 3 Points.

_____ Port Security Manager, Trained Port Security Personnel, Fully Equipped: 1 Point.

_____ Port Security Manager, Trained Port Security Personnel, Fully Equipped, Security Exercises Conducted Regular Schedule: 0 Points.

3. Physical Security: (12 points).

COMMENT: The following factors should be considered when assigning point values: Barriers, Fencing, Lighting, Vehicle Barriers for critical pier areas and Entry Control.

_____ Security Systems (Landside)

No Systems: 4 Points

Some Systems: 2 Points

All Systems: 0 Points

3. Physical Security: (Cont.)

Comment: The following factors should be considered when assigning point values: Patrol Craft, Surveillance Systems, Surface Search Radar, Anti-Swimmer Sonar, Barriers/nets, and Magnetic loop detector/other sensor for submerged delivery vehicles (SDV)

_____ Security Systems (Waterside)

No Waterside Security: 6 Points

Waterside Lighting Only: 5 Points

Live Surveillance Only: 4 Points

Some Technical Surveillance: 3 Points

All Combined Technical Systems only: 2 Points

All Technical Systems with Live Surveillance: 1 Point

All Technical Systems with waterside lighting and live surveillance: (0 Points)

COMMENT: Terrain within 1 mile should be analyzed in conjuction with a review of port facility sensitivity, adequacy of barrier fencing, and access/egress route analysis.

_____ Terrain

Built up, Commercial: 2 Points

Mountainous, Forested, Undeveloped: 1 Point

Open Clear area: 0 Points

4. Routes of Access and Egress: (9 Points).

_____ Roads.

Expressways: 3 Points

Major Hiways: 2 Points

Congested city streets: 1 Point

4. Routes of Access and Egress: (Cont.)

_____ Rail.

Rail Gates Open at all Times: 3 Points

Rail Gates Open when in Use: 2 Points

Unused Rail Access: 1 Point

No Rail Access: 0 Points

_____ Water Channels.

More Than 3 Choke Points: 3 Points

1-3 Choke Points: 2 Points

No Choke Points: 1 Point

5. Communications: (10 Points).

COMMENT: Consideration should be given to secure lines of communication. Consultation with the appropriate port authority personnel and local, provincial, and federal law enforcement personnel is required to accurately reflect vulnerability and operational effectiveness.

_____ Compatible Communication by Port Authority with:

Local Law Enforcement Agency only: 4 Points

Provincial and Local Law Enforcement Agencies: 2 Points

Federal, Provincial, and Local Law Enforcement Agencies: 0 Points

_____ Landline Telecommunications.

Non-Dedicated: 4 Points

Dedicated Point-to-Point: 2 Points

Secure Dedicated: 0 Points

_____ Radio Communications

Non-Dedicated: 2 Points

Dedicated: 1 Point

Secure Dedicated: 0 Points

6. Sustainability of Additional Port Security Resources (8 Points)

_____ Port Security Law Enforcement Resources.

Threat	Sustainability (Days)			
	1	3	7	Indefinite
High	8	6	4	2
Medium	7	5	3	1
Low	6	4	2	0

Threat Definitions:

High: Intelligence indicating an attack of some type will occur within the port.

Medium: Intelligence indicating an attack of some type may occur within the port.

Low: Any other intelligence indicating the possibility of terrorist/subversive activity.

7. Response Time for Security Personnel Capable of Rendering Emergency Assistance: (7 Points)

_____ Response to Attack: (4 Points)

Response Force	Time to Respond (minuntes)		
	30	30-60	60+
Patrol	2	3	4
Bomb Squad	1	2	3
SWAT	0	1	2

_____ Response to Accidents/Fire: (3 Points)

Response Force	Time to Respond (minutes)		
	15	15-45	45+
Fire Department	1	2	3
Pollution Response Team	0	1	2

COMMENT: Coordination should be made with all agencies capable of rendering assistance. Plans should be developed and tested to determine response time and level of capability.

8. Time/Proximity to Urban Areas: (7 Points)

_____ Port is surrounded by and contiguous to a heavily populated urban area of over 100,000 people. (7 Points)

_____ Port is surrounded by an area populated by 50,000 to 100,000 people. (6 Points)

_____ Port is surrounded by an area of less than 50,000 people and the nearest city of greater than 100,000 people is less than 20 miles away. (5 Points)

_____ Port is surrounded by an area of less than 50,000 people and the nearest city of greater than 100,000 people is 20 to 50 miles away. (4 Points)

_____ Port is surrounded by an area of less than 50,000 people and the nearest city of greater than 100,000 people is 50 to 100 miles away. (3 Points)

_____ Port is surrounded by an area of less than 50,000 people and the nearest city of greater than 100,000 people is more than 100 miles away. (2 Points)

_____ Port is isolated and surrounded by rural undeveloped countryside. (1 Point)

9. Local Social Environment. (8 Points)

_____ Points

California/ OCONUS	8 Points
East Coast	6 Points
Gulf Coast	4 Points
Northwest, Central and Northeast	2 Points

COMMENT: Points are awarded based on historical data gathered on terrorist/subversive activity by geographic region. Special attention should be give to monitoring social unrest/demonstrations in the local areas.

10. Proximity to International Borders: (3 Points)

COMMENT: For Current Threat Level, Refer to Question 1. If no Threat Assessment is available assign 3 points

_____ High Threat Area.

0-100 miles: 3 Points

101-500 miles: 2 Points

+500 miles: 1 Point

_____ Medium Threat Area.

0-100 miles: 2 Points

101-330 miles: 1 Point

+500 miles: 0 Points

_____ Low Threat Area.

0-100 miles: 1 Points

101-500 miles: 0 Points

+500 miles: 0 Points

_____ Islands: 0 Points

****

RANGE OF VULNERABILITY

Very Low	Low	Medium	High	Very High
0-10 pts	11-30 pts	31-55 pts	56-75 pts	76-90 pts

APPENDIX 3

R 231925Z DEC 86

FM COGARD INTELCOORDCEN WASHINGTON DC

Subj: TERRORISM THREAT ASSESSMENT SERIES

1. As part of this command's mission in support of Coast Guard programs, ICC provides terrorism/security-related situational and locational threat assessments. These assessments, produced on a scheduled (4-6 week interval, generally) as well as specific request basis, are intended to assist Coast Guard commands in evaluating foreign travel, port calls and security issues associated with Coast Guard pers/facilities.

2. ICC assessments are prepared from intelligence reports and documents received from/thru the national intelligence community and are updated/amplified through consultations with analysts from those agencies. These reports/consults are further supplemented with information obtained during intelligence agency meetings and working groups (e.g., National Intel Officer for Counterterrorism, Interagency Intel Committeee on Terrorism). The agencies from which we draw this information include, but are not limited to: CIA, DIA, NSA, Navy Anti-terrorism Alert Center (ATAC), Army Intelligence and Threat Analysis Center (ITAC), Military Airlift Command Intelligence Center, Departments of State and Treasury, and the Drug Enforcement Administration. (Note 1: each agency has its own focus and qualitatively defined levels of threat; thus, their respective assessments of threat levels can and do vary). (Note 2: State Department (Consular Affairs and Citizens Emergency Center vice Dept's intel or security elements) regularly provide travel advisories for use by the general public. These advisories are generally cautionary in content and frequently do not reflect matters applicable to USG official travel. For example, the general public advisories for Columbia and Peru caution citizen travel to certain in-country areas. On the other hand, Columbia has been officially designated as a hostile fire area, for which eligible USG reps have been authorized to receive hostile fire pay or equivilent. As for Peru, the U.S. Ambassador has directed that official travel to/in country must be justified on a real/high need basis and that USG reps should not be surprised if the response to their "country clearance" request is a denial of travel clearance).

3. Content of the ICC terrorism threat assessment series is based upon essentially the same info held by national intel elements and reflects the general thrust/spirit of community members' assessments. However, ICC assessments are tailored to reflect/respond to COGARD interests/work environment and, therefore, do not necessarily conform with individual agency threat levels. In preparing our assessments, we take into consideration military, security, political, cultural, and economic matters--current and historical--associated with the area in question which may impact on COGARD missions. Our assessments, like those of the other intel orgs mentioned, are in no way intended to persuade/dissuade travel to a given area nor are they intended to stand as USG/USCG policy or formal national intel community products.

4. ICC assessments are qualitative and use a five point scale, similar to that used by other agencies: low, low-to-moderate, moderate, moderate-to-high, and high. The assignment of one of these levels is determined by analyzing all available intel info. Relevant factors considered include, but are not limited to, the following essential elements of information (EEI):

A. The presence of known terrorists (indigenous to the area or international in nature) in the country/area in question;

B. Terrorist operations conducted in-country in the past;

C. Whether or not a terrorist network/infrastructure is established in the area;

D. Whether there has been any reported targeting of U.S. interests (e.g. officials, citizens, govt/non-govt facilities);

E. Assessments as to whether or not the terrorist groups in the area have demonstrated the capability and/or intention to carry out terrorist operations;

F. Whether or not there are any specific threats to COGARD personnel or facilities, or threats associated with COGARD missions (e.g. maritime law enforcement v. narcotrafficers);

G. Historical cultural, political situations which are germane to the current situation; and

H. The extant security situation.

5. This message is intended to inform users of ICC terrorism threat assessments and their formulation process so as to aid you in making well informed operational decisions. Such products will not address whether or not a specific travel plan should be carried out. The threat assessment is simply one factor which can and will provide our evaluation of the intelligence information which has comprised the basis of the assessment. A determination that a locale is assessed as 'high threat' does not necessarily mean that travel must not be made to that area nor does one which concludes 'low threat' automatically mean that travel should be made. Each decision should be made on its own merits with full consideration for the facts on hand and the extant situation (re. purpose and relative need for travel, implications of 'go/no go' decision, etc.).

6. ICC produces two routine products which we would like to bring to your attention. As other requirements permit, we produce a foreign locales terrorism review/assessment on a monthly/bi-monthly basis. In addition, on a routine basis and scheduled in between the foreign assessment, we produce a domestic threat assessment/review. The most current of each of these should be your first reference source for information on specific areas of the world/U.S. They are intended to serve as standing information for your use and we will reference them as the information baseline in our amplified response to as specific area/time assessment request. In addition to these scheduled reports, we are prepared to send 'spot' reports in response to special situations (known or projected) or a 'travel alert' or 'travel advisory' issued by the national intelligence community. All classified ICC threat assessments/reports are addressed to area/district intel offices for further dissemination to COGARD field commands as appropriate.

7. Wth regard to requests for special/specific threat assessments ICC shall make every effort to provide a timely response. However, commands must keep in mind that the process of multi-source contact, info collation, evaluation and analysis, and preparation for transmission is both person-power and time consuming. The broader the request--vis-a-vis--locale(s), itenerary, activity, etc.--the more complex the assessment process. Accordingly, commands are urged to communicate (e.g., phone with message confirmation) their desire for a threat assessment as soon as the specifics of the situation are known or can be reasonably projected. Inasmuch as there is much on the ICC mission menu and a dynamic priority setting environment, an indication by the requesting command of target date or situational exigency would be helpful also.

FOREIGN PORT FACILITY SECURITY SURVEY

APPENDIX 4

A. Access to the Port Facility:

1. Is vehicular and pedestrian traffic to the port facility area controlled or monitored sufficiently by port security personnel so that unauthorized entry of vehicles or personnel would not go undetected?

2. Are waterways to the port under sufficient observation by port security personnel so that unauthorized small watercraft and surface swimmers would be detected and prevented from approaching docks and docked passenger vessels?

B. Access to Dockside:

1. Do dock areas have adequate fencing or other barriers to separate them from the street and from other public areas?

2. Are dock areas illuminated adequately at night?

3. Are dock areas patrolled regularly?

4. Do guards control entrances and exits?

5. Are vehicles, persons and property screened before being permitted to proceed beyond access points, to include vendors, contractors, service and miscellaneous personnel.

6. Are ship stores or cargo opened or x-rayed before being loaded?

C. Access to Passenger Terminal:

1. Are security barriers used to control and channel passengers into a restricted/secure area?

2. Are the barriers sufficient in height and durability to deter or delay unauthorized passage?

3. Are the passengers and visitors controlled and monitored in the resticted/secured area?

4. Do port facility employees display identification badges?

5. Are vendors/service/repair personnel required to display identification badges, and are their movements controlled?

6. Are metal detectors, electronic devices, manual searches or other means used to screen person seeking entry to the restricted/secure area?

7. Is baggage/personal property visually inspected or electronically screened before being loaded onto the ship?

8. Is the terminal area illuminated adequately?

9. Are security barriers used to channel passengers from the restricted/secure area to the ship?

10. Are port security personnel stationed at the ramp?

D. Port Security Force:

1. Are port security personnel supplemented by local law enforcement or military/paramilitary personnel?

2. Do personnel responsible for security inspections appear competent and well-trained?

3. Are they armed?

4. Are they equipped with two-way radios?

5. Are communcations adequate to quickly contact local police in the event of an emergency?

6. Do port security personnel or police have the training and equipment to recognize dangerous substances and devices?

7. How quickly could additional police or security reinforcements respond to a port emergency?

8. Is there a port emergency plan which covers terrorist incidents?

9. Are port emergency/security exercises conducted regularly?

10. In your estimation does the port security force appear to be able to detect or deter unauthorized access to port/terminal/ship by a person or group, with lethal devices, intent upon takeover of a passenger vessel or doing harm to passengers?

E. Surveying Officer's Comments/Conclusions Regarding the Effectiveness of Port Security Measures. (A short narrative covering the strengths and weaknesses of physical and procedural security measures at the surveyed port).

RONALD W. REAGAN LIBRARY

THIS FORM MARKS THE FILE LOCATION OF ITEM NUMBER 1 LISTED ON THE WITHDRAWAL SHEET AT THE FRONT OF THIS FOLDER.

RONALD W. REAGAN LIBRARY

THIS FORM MARKS THE FILE LOCATION OF ITEM NUMBER 2 LISTED ON THE WITHDRAWAL SHEET AT THE FRONT OF THIS FOLDER.

In response to the recommendation of the Vice President's Task Force, the Department submitted legislation authorizing access by airport authorities to criminal history data. The proposal received a generally negative reaction and neither House even scheduled hearings. The proposal died at the end of last Congress. Because of the negative reaction the Department has not resubmitted the proposal.

Jim Nichol provided this for our information. He's still pursuing industry efforts to thwart domestic terrorist incidents.

B.
Fill VP Task Force
R Scot

Nuclear Proliferation: Studies and Strategies for Stopping the Spread of the Bomb

NUCLEAR CONTROL INSTITUTE
1000 Connecticut Avenue, N.W., Suite 704 Washington, D.C. 20036 (202) 822-8444

Iranian Threat Against U.S. Nuclear Reactors

October 17, 1987

The Honorable Frank C. Carlucci III
Assistant to the President
for National Security Affairs
The White House
Room 1/WW
Washington, D.C. 20500

OCT [illegible]

Dear Mr. Carlucci:

At this time, while planning is under way in the U.S. Government on possible responses to Iran's Silkworm-missile attack on a U.S.-flagged oil tanker, we believe it to be imperative that you consider the potential catastrophic consequences implicit in a threat made recently by Iran. The threat was directed against U.S. nuclear reactors in anticipation of the type of confrontation that exists today.

On June 9, 1987 according to an Associated Press report on a Radio Teheran broadcast monitored in Nicosia, the Iranian government responded to the possibility of U.S. strikes against the Silkworm missile batteries by warning that "U.S. centers and nuclear reactors can be more vulnerable than the missile bases of the Islamic Republic of Iran." ["Iran-US," AP-WX-06-10-87 1006 EDT]

The NRC promptly notified all power and research reactor and fuel-facility licensees of "information received that could be a vague threat to U.S. nuclear facilities" and of its conclusion, after contacting other government agencies, that "licensee action in response to this information is not warranted at this time." ["Iranian Official Implies Vague Threat to U.S. Resources," NRC information Notice No. 87-27, June 10, 1987]

It should be of concern to you that the Nuclear Regulatory Commission does not require protection of licensed U.S. nuclear reactors against [redacted] even though a study conducted for the NRC by Sandia National Laboratories in early 1984 concluded, according to an NRC unclassified summary, that ". . . unacceptable damage to vital reactor systems could occur from a relatively small charge at close distances and also from larger but still reasonable size charges at large setback distances

(greater than the protected area for most plants)." ["Weekly Information Report to the NRC Commisioners," April 20, 1984, describing "Analysis of Truck Bomb Threat for Nuclear Facilities" by Leon D. Chapman and David E. Bennett, Sandia National Laboratories, February 21, 1984] A peer review conducted for the NRC by the Naval Ordnance Laboratory found that the Sandia report was "generally correct with a moderate level of conservatism in the consequence predictions," according to an NRC staff report ["Truck Bomb Threat," Memorandum for John G. Davis from Robert F. Burnett, August 14, 1984]

The Sandia and Naval Ordnance assessments lend support to a recommendation of the International Task Force on Prevention of Nuclear Terrorism that "Power reactors should be protected against vehicular threats." In its June, 1986 report, the Task Force stated as follows: "The size of exclusion zones at nuclear power reactor sites should be reexamined to ensure that the zones are large enough to neutralize the possible catastrophic consequences of a truck bomb set off at the perimeter fence. All reactor sites should be modified promptly with barriers to shield critical areas of the plant against potential consequences of truck bombs set off on-site. This may require revising the design-basis threat to include protection against vehicular access---a requirement not included in U.S. licensing regulations, for example." [Preventing Nuclear Terrorism--The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism, A Nuclear Control Institute Book, Lexington Books, 1987, p. 22]

We have enclosed a paper, "Severe Accidents and Terrorist Threats," by Gerald L. Pollock, professor of physics at Michigan State University, who served as a consultant to the Task Force on the issue of potential consequences of terrorist acts against nuclear power plants. [Preventing Nuclear Terrorism, pp. 66-77] We urge you to review this paper with the understanding that a truck bomb can destroy the control room and some of the essential plumbing of a nuclear powerplant.

Iran may make threats on which it does not follow through; and the official U.S. Government assessment apparently is that the Iranian threat against U.S. reactors is not now credible. We believe, nevertheless, that the known vulnerability of U.S. nuclear reactors to explosions of truck and other vehicular bombs, and the extremely severe consequences that could result from a successful attack, warrant Iran's threat against U.S. reactors being taken seriously at this time.

Accordingly, we urge you, in conducting the ongoing review of options and contingencies arising from the current situation in the Persian Gulf, to examine the need for an immediate state of alert and for prompt action to [redacted] and other precautions at U.S. reactor and other nuclear sites [redacted]-

bomb attack. We believe this action is needed as a matter of prudence, even in the absence of an official assessment of an existing threat because, should the threat assessment change, there might not be sufficient time adequately to protect these facilities from vehicular-bomb attack. At a minimum, remedial measures should be undertaken at nuclear power plants and research reactors located close to or within major population centers.

We thank you for your consideration of this urgent request. We are prepared to make available to you the considerable expertise of the Task Force and its consultants.

Sincerely,

Paul Leventhal
President

Milton Hoenig
Scientific Director

Enclosure

Severe Accidents and Terrorist Threats at Nuclear Reactors

Gerald L. Pollack

Is it possible to predict accurately what radioactive releases might occur in the event of a severe accident at a nuclear reactor, such as terrorist actions might bring about? In fact, the kinds of damage that a terrorist attack could cause are similar in many ways to that which could result from a reactor accident occurring during normal operations. The actual consequences will depend on what access the terrorists have to critical parts of the reactor (such as the auxiliary building, turbine building, control room, and containment), on the specific nature of the damage they do, and on what remedial actions the reactor operators can take. If the damage is limited to one function or one component of the reactor (such as a loss of coolant from the primary or secondary systems or interference with the external electric power supply to the reactor), then the consequences may be kept small by remedial action of the operators and by built-in engineered safety features. But if the damage affects several reactor components (such as the primary or secondary coolant systems and emergency backup coolant systems, or a cutoff of the external AC electrical power and of the internal backup DC power) or if no remedial action can be taken, then the consequences can be considerably more severe, even after a "scram," that is, an emergency shut down.

In severe accidents, the containment vessel plays a critical role in limiting the consequences. Thus the key defense against major radioactive emissions to the outside is to keep the containment intact as long as possible. For this reason, containment vessels are built with several safety devices, such as containment sprays, hydrogen igniters, and ice condensers. If a terrorist action were to damage the containment severely, especially in the early stages of the attack, then an accident would likely result in greater radioactive emissions to the outside.

Many kinds of reactor accidents have been studied by the U.S. Nuclear Regulatory Commission (NRC) and by the academic and industrial communities. The main study has been conducted by the NRC. The report, referred to as NUREG-0956, considers sixteen different modeled accidents at five reactors.[1] The American Physical Society (APS) has also written a report on severe accidents at nuclear power plants in the context of NUREG-0956,[2] and there have been complementary studies of this problem by the American Nuclear Society as part of the Industry Degraded Core Rulemaking Program (IDCOR) sponsored by the Atomic Industrial Forum.[3] The consensus of the technical community is that a lot more is now known about what happens in a reactor accident and what the consequences of different accidents would be than was true before NUREG-0956, but that there are still many important uncertainties in what is known and much that is still not known.

Some of the key areas of uncertainty are the nature of the physical and chemical interactions of released fission products and of the interactions between a molten core and concrete, the completeness and validity of the computer codes used to predict accidents, and the behavior of the containment. Because of these and other uncertainties, it is not yet possible to reliably predict the consequences of reactor accidents. It is known that for many accident scenarios, especially less severe ones or where the containment is not seriously compromised, the amount of radioactive material expected to escape the reactor is less, even much less, than was previously calculated. For such accidents, the predictions are easier and more reliable. With severe accidents, however, there is considerable uncertainty as to the predicted results. For accidents of the type that terrorists might cause—for example, where the sequence of failure would be unexpected or where redundant safety features are caused to fail together—the uncertainties are still larger.

The conclusion, then, is that there are potential dangers to the public from terrorist actions at a nuclear reactor; however, because of the variety of potential terrorist threats and the incompleteness of the knowledge about the behavior of reactor components and fission products during accidents, the consequences cannot yet be assessed quantitatively.

Behavior of Nuclear Reactors during Accidents

The best way to learn about nuclear accidents is to study the ones that have taken place in terms of emissions, debris, reconstruction of events, and other factors. The most complete study of nuclear reactor accidents and their consequences is summarized in the NRC's NUREG-0956.[4] (There have been earlier studies of this problem, in particular, the Reactor Safety Study, WASH-1400, of October 1975.) The major impetus for the NRC's recent study was the Three Mile Island (TMI-2) reactor accident in March 1979. It resulted in emissions of radioactive materials of about 10^7 curies of noble gases, mainly xenon 133, and about 17 curies of iodine 131, much less than had been

expected for an accident of its kind. The study was undertaken to learn more about the behavior of fission products and reactor components during severe reactor accidents so that previous regulatory assumptions could be reassessed.

The APS report lists, besides TMI-2, fourteen accidents and associated radioactive emissions from 1952 to 1979. Of these, the most serious in terms of consequences to the public was a fire at the Windscale reactor in England in 1957. The emissions from that accident have been estimated to have included about 3×10^5 curies of noble gases, 18,000 curies of iodine, and about 13,000 curies of radioactive metallic elements. Many more nuclear reactor accidents are mentioned in a recent report of the General Accounting Office, which noted 151 "significant nuclear safety incidents" in "unnamed Western countries." Few details are known about these accidents.

Of the several other accidents at nuclear reactors, none has been studied as thoroughly and well as TMI-2. NUREG-0956 brought together the results of experiments and analyses of people at the NRC, Oak Ridge National Laboratory, Sandia National Laboratories, Idaho National Engineering Laboratory, Battelle Columbus Laboratories (development of computer codes and analysis), and others and is the result of several years' work. The sixteen severe accidents analyzed involved, for example, loss of coolant and loss of AC power, a pipe break with a failure of the emergency core cooling system, stuck-open valves, unavailability of containment safety features, and containment failure. The five reactors for which these kinds of accidents were modeled are different and representative types. The Surry, Sequoyah, and Zion facilities have pressurized water reactors; the Peach Bottom and Grand Gulf facilities have boiling water reactors. All these reactors have different containment structures and vary in other details as well.

Many of the uncertainties of the consequences of reactor accidents and a lot of gaps in knowledge are noted in NUREG-0956. The impact of even modeled nuclear accidents cannot yet be predicted satisfactorily, let alone that of accidents caused by a large-scale terrorist attack. However, it is important to emphasize that NUREG-0956 offers the best knowledge there is on the subject and is an important and strong step toward greater understanding.

Major Areas of Uncertainty

The studies of severe reactor accidents recognize many areas in which there are important uncertainties. NUREG-0956 lists eight, the APS report makes eighteen recommendations for future research, and the American Nuclear Society report lists eight topics that require additional investigation. Additionally, there are eighteen technical issues on which differences exist between the NRC and IDCOR, and many areas of uncertainty are discussed in

the comments of the Advisory Committee on Reactor Safeguards.[6] Nevertheless, these reports agree on several areas of uncertainty: interactions of fission products in the reactor pressure vessel and containment, core melting, interaction between molten core and concrete, containment response and failure, and validation of the computer codes used to calculate accident consequences.

Nuclear Reactor Operation

As background to a closer look at the areas of uncertainty, it is useful to review how a reactor works. The source of the energy in a nuclear reactor comes from the fissioning of the uranium fuel. In this process, a neutron impinges on (hits) a uranium nucleus (the isotope uranium 235), which then fissions (splits) into other chemical elements (fission products) and two or three neutrons. Most of the energy of this process (168 million electron volts, MeV, out of a total of 212 MeV) is carried off as kinetic energy of the fission products. About 7.5 percent appears as radioactive decay of the fission products, a process of decay that continues to be a source of heat even after the reactor has been shut down; therefore that heat plays an important role in accidents. Because the physics of fission and fission product decay is well understood, it is possible to know the composition of the core of a reactor reliably after it has been running. For a typical operating pressurized water reactor, the core contains hundreds of millions of curies each of noble gases (krypton and xenon), iodine, alkaline earths (strontium and barium), volatile oxides (cobalt, molybdenum, technetium, and ruthenium), and nonvolatile oxides (lanthanides and actinides), as well as tellurium and antimony.

During normal reactor operation, these fission products are retained, with the unspent fuel, within the cladding that surrounds the fuel rods. This cladding is an alloy of zirconium and is normally leak-tight. The main danger in a nuclear reactor accident is that these radioactive fission products will leak past the cladding and ultimately end up being emitted outside the reactor. The amount, kind, and timing of radioactive emissions to the environment from a nuclear accident are collectively called the source term.

The energy of uranium 235 fission is carried away from the core by a large amount (about 190,000 kilograms) of rapidly flowing (46 million kilograms per hour) water under high pressure (2,300 pounds per square inch). This water, which is contained in the reactor pressure vessel and associated tubing, comprises the primary coolant system. Its role is to keep the fuel from melting, as well as to transport energy in the form of heat. In normal operations, the fission products are isolated from the self-contained primary coolant system, which in turn is isolated, inside a large reactor containment, from the outside.

Useful energy is normally transported outside the reactor by a secondary coolant system that provides steam to turn the turbines that drive the electric generators. The thermal contact between the primary and secondary coolant systems takes place in heat exchangers (steam generators) inside the containment; however, the flow paths of primary and secondary coolant systems are separate, and there is no intermixing. In a typical pressurized water reactor—say, the Surry reactor—the total power that is thermally generated in the core is 2,400 megawatts, and the reactor's electrical power output is 800 megawatts. Thus, the efficiency of the conversion from thermal to electrical power at Surry is about 30 percent.

Emissions of Iodine and Other Volatile Fission Products

Because of their biological importance, emissions of radioactive iodine have always been a major interest in assessing the danger to the public from reactor accidents. At the same time, a major source of the current uncertainty in predicting the consequences of reactor accidents is the lack of understanding of the emission, retention, and general interaction of iodine and other volatile fission products during reactor accidents.[7]

Iodine is one of the more volatile elements in the radioactive inventory of a reactor; thus it is one of the first fission products released from the core if the fuel overheats and the cladding breaks. The environmentally important radioiodine isotope is iodine 131, since it decays with a comparatively long half-life of eight days; the other emitted iodine isotopes decay much more rapidly. (Half-life is the time it takes for half of a radioactive isotope to decay. In eight days, half the iodine 131 decays to nonradioactive xenon.) Radioactive iodine is biologically dangerous because it enters the body by inhalation and by ingestion of milk; it concentrates in and damages the thyroid gland. Some other volatile elements that are released early in an accident are xenon, krypton, cesium, and tellurium.

In the TMI-2 accident, the amount of iodine 131 emitted was remarkably small; only about 17 curies out of an estimated inventory of 64 million curies were emitted. It is thought that most of the iodine was retained in soluble form in the water inside the damaged reactor. The theory is that the reactor atmosphere during the accident was reducing (rich in steam, hydrogen, and water but poor in oxygen) and that this circumstance favored reactions that formed water-soluble metallic iodides. In the Windscale accident, by contrast, about 18,000 curies (about 10 percent of the inventory) of radioiodine escaped, probably because the chemical environment was different.

The source of the uncertainty in determining how much of a given fission product will be emitted, how much will be retained, where it will be retained, and other parameters is that each fission product has its own chemical and physical properties. The situation is simplest with the inert gases, which do not react and cannot condense in a reactor. For iodine and other elements, the situation is more uncertain because of the large number of interactions and variety of molecular products they can form. Iodine, for example, can exist in several volatile (gaseous) forms, such as molecular iodine, hydrogen iodide, and organic iodides (such as methyl iodide). Volatile forms of radioiodine are naturally emitted from reactor accidents more easily than condensed iodine compounds.

The chemistry of iodine in the atmosphere of a damaged reactor is complicated, a fact that makes the problem of predicting radioiodine emissions from a reactor accident uncertain. For example, the origin of organic iodides is not known (although they are probably the result of interactions between fission product iodine and organic lubricants, and other organic compounds). Inside a severely damaged reactor, the radiation fields may be intense (typically 1 megarad per hour), and the radiation itself can strongly affect chemical interactions. Recent experiments at Oak Ridge National Laboratory have shown that irradiation enhances the formation of organic iodides, some of which are volatile.

Iodine can also form cesium iodide by combining with the fission product cesium. This compound is water soluble and so provides a mechanism for the retention of iodine. Recent experiments at Sandia National Laboratories show that volatile iodine is released when cesium iodide comes into contact with the alloy Inconel. Calculations at Battelle Columbus Laboratories have shown that even nonvolatile compounds that have condensed can be revolatilized by the heat from fission product decay.

In short, the chemistry of iodine in a reactor is important to understand, yet knowledge about it is sparse. (I have gone into so much detail on iodine because it is such an important contributor to dose consequences.) It is probably fair to say that for any reactive fission product, the chemical reactions that can take place in the atmosphere of a severely damaged reactor are not understood. More large-scale experiments are needed in which interactions among many different atoms and molecules in the required variety of atmospheres, pressures, temperatures, and radiation fields are studied. That kind of understanding is years in the future.

Melting of the Core

If the primary coolant does not carry off enough energy, the core will melt, and fission products will be released from it into the reactor pressure vessel. There are several uncertainties as to what happens then. In NUREG-0956, the NRC notes uncertainties relating to "natural circulation in the reactor vessel" and "core melt progression and hydrogen generation." The APS report refers to "damage progression in the core," and the American Nuclear Society report cites as areas requiring additional investigation the "mechanisms of

core degradation," "aerosol transport," and "thermal hydraulics" in the reactor coolant system.

Nuclear reactors are designed to withstand, without melting the core or breaking the containment, a so-called design basis accident: loss of coolant accident. In this accident, there is a sudden, double-ended break of the largest pipe in the reactor's primary coolant system. Built into the reactor coolant system are several safety features that would remove heat from the core if the main primary coolant circulation system were to fail. The more serious accidents occur when these backup systems fail, and the core melts. Two of the emergency coolant systems that come into play are a passive system that floods the core with borated water if the primary coolant pressure drops, and emergency coolant pumps, some of which drive water at high pressure and others of which drive large volumes of water at low pressure, with some of the pumps actively driven by electric power and some by steam. To cause a severe nuclear accident, a terrorist attack would have to damage or otherwise render inoperative both the backup systems and the main primary coolant system.

The first line of defense against a severe accident is to scram, or shut down, the reactor by rapidly lowering the control rods that absorb neutrons and thereby stopping the fission reaction. Nevertheless, decay heat is still generated in the core. In a 3,000 megawatt thermal reactor, that decay heat is initially about 225 megawatts, and from the viewpoint of accident management, it is important to keep sufficient primary coolant flowing even after a scram; otherwise the fission product decay heat will lead to core melt. A key factor in a core melt is that when the temperature reaches about 1,000 degrees centigrade, the zirconium of the cladding interacts with water and steam or oxidizes, an exothermic process that also produces heat, which eventually will melt the core. The oxidation also produces hydrogen gas, a potential threat to the containment. Thus, in the case of a terrorist threat, it would not be enough to shut down the reactor; the operator would also have to ensure that the core was supplied with coolant for about a week to ten days.

If the primary and backup coolant systems fail, the core will melt, and fission products will be emitted into the reactor pressure vessel in ways that are not well understood. For example, not enough is known about core temperatures[8] or about the order, rates, and kinds of damage that occur in the core.[9] Nor is enough known about the circulation patterns[10] and the thermal and flow conditions[11] that transport the fission products through the reactor pressure vessel, in particular, in the upper plenum of the vessel.

These fission products are transported as vapors and as aerosols through the primary system, including the piping and steam generator. More needs to be known about the makeup of these aerosols and where they ultimately wind up in the reactor. There are also uncertainties about what happens to

the control rod materials (silver, indium, and cadmium).[12] A potentially important source of emissions is revolatilization of fission products because of fission product self-heating.[13] The Advisory Committee on Reactor Safeguards has pointed to the problem that fission products may be deposited in the steam generator tubes, as well as in the upper plenum, where their decay heat may rupture these surfaces and provide important escape routes for radionuclides out of the primary system.[14]

Interactions of a Molten Core and Concrete and Behavior of the Containment

If a severe reactor accident proceeds to the point at which the core melts and slumps to the bottom of the reactor pressure vessel, the potential consequences become much greater. The crucial stage would be when the core melts through the bottom of the pressure vessel and drops into the water and onto the concrete basemat of the reactor cavity. This event is the ex-vessel phase of the accident; fission products and molten core are released into the containment, a release that is accompanied by large pressure and temperature increases in the containment environment. The subsequent development and outcome of the accident depend in important ways on what specifically happens during the core-concrete interaction and on how the containment vessel behaves under these pressure loads. It is necessary to know whether the containment holds or fails and, if it fails, when and how.

The physical and chemical interactions in this phase of an accident are complex, and much is not understood. The source of the complexity is that there are many chemical components (perhaps 28 elements in the core debris, 13 compounds in the concrete, and, according to one computer code formulation, 137 vapor species) in a multiphase (gas, liquid, and solid) mixture at high temperatures. The interactions among these components depend critically on temperature, but the temperature distribution is not known. For some processes, the release of fission products is an exponential function of temperature; that is, relatively small changes in temperature lead to large release effects.

One of the areas of uncertainty is how fission products are released and how aerosols are generated in the core-concrete interaction.[15] A particularly important question on which more research is needed is how refractory radioactive materials such as lanthanides and actinides (including plutonium) are released.[16] The amounts of these elements (some of which are biologically active) that are released are sensitive to the temperature, but the thermal hydraulics of the core-concrete interaction are not well understood.[17] When the molten core interacts with the concrete, the latter decomposes thermally and releases steam and carbon dioxide. These gases sparge up through the molten core at temperatures above 2,000 degrees centigrade and pick up

and transport into the containment in aerosol form many nonradioactive and radioactive materials.

The containment is the most important barrier to large releases of fission products. If the containment stays intact for days, or even for several hours, following a severe nuclear accident, the dose consequences to the environment are much reduced over what they would be if the containment were breached early in an accident. The reports of the NRC, the APS, and the American Nuclear Society all point to the problems of containment pressure loads, leakage, and failure as areas of major uncertainty or that require additional research.[18] Containment performance is also one of the technical issues on which the NRC and IDCOR differ.[19] Finally, the Advisory Committee on Reactor Safeguards concluded that a "much less ambiguous method for taking account of containment performance is needed."[20]

In a severe reactor accident, the challenge to the integrity of the containment is great because of the increase in pressure resulting from fission product heat, zirconium oxidation, gas generation, and other areas as the molten fuel is discharged into the containment. Because at this point the containment atmosphere contains many fission products in vapor and aerosol form, it is the worst time for failure. For most modeled pathways, sprays and other mitigating safety features keep the containment intact for hours, days, or indefinitely. There is one important sequence, however, technically known as the beta sequence, in which there is a preexisting or early failure of the containment that allows the discharge of fission products. In this case, the size of the breach in the containment is an important parameter. If the failure consists of small holes (for example, failed seals, gaskets, valves, or one of the other many small containment penetrations), the release may not be serious. However, if a large equipment hatch is left open or if the containment has a large hole because of terrorist actions, the emissions of radioactivity out of the reactor may be large.

One reason why there are substantial uncertainties as to containment behavior is that there are many kinds of containments (with different safety systems, penetrations, and geometry), and they are all large (a typical pressurized water reactor containment has a volume of about 60,000 cubic meters). It is therefore difficult to conduct realistic containment experiments. There have been tests of containment failure at Sandia National Laboratories, and more are underway through the NRC and the Energy and Power Research Institute. Eventually much more will be known about this problem.

Computer Codes for Predicting the Consequences of Reactor Accidents

In the NRC reassessment program, predictions of the consequences of nuclear reactor accidents are generated by specialized computer codes.[21] These codes

are the core of the NUREG-0956 program in the sense that they use all the theoretical and experimental data available as the basis for modeling the important phenomena that determine releases from an accident. As an example, if the postulate is an accident that involves a transient event with failure of the relief valves and of the power conversion and feedwater systems, as well as a station blackout (this sequence is called TMLB'), the inputs into the computer code include these accident conditions and the parameters of the particular reactor at which the accident is postulated to occur. The output of the code is a description of the course of the accident and its consequences: for example, when the core will become uncovered, when the molten core will attack the concrete, what thermal and pressure conditions the reactor will experience, and, depending on the behavior of the containment and on how complete the modeling is, the nature and timing of fission product releases to the environment.

There are many difficulties in developing codes that predict reliably the consequences of such complicated sequences of events. The most complete, critical analysis of the codes is in the APS report. Many people in the research community feel that the codes need a lot of improvement before they produce reliable conclusions.[22]

Accident sequences are analyzed by a series of codes so that the output of one serves as the input to the next code (or to several codes). For example, all the analyses start with a computer code calculation of the fission products present in the core when the accident starts. These data serve as the input to a series of codes that calculate the thermal hydraulics (temperature, pressure, and flow) in the primary system of the reactor and to a code that calculates fission product releases from the molten fuel. Subsequent codes calculate the transportation and deposition of fission products, the products of core-concrete interaction, the production of hydrogen and other gases, and the behavior of aerosols airborne in the containment.

The APS report points out that the result of these codes are uncertain because some important phenomena are omitted while other important phenomena are modeled crudely and because the codes are sensitive to the lack of complete data. It is always necessary to use simplifying assumptions in computer calculations of physical phenomena in order to keep the problems tractable. However, the results calculated on the basis of simplified assumptions may not correspond well to reality. One important simplification that present codes make is to assume that flow is one-dimensional rather than using a proper model of the natural circulation in the reactor pressure vessel. Large uncertainties are present in the code results because of a lack of knowledge of how the core melts and slumps and of how core fragmentation and heat transfer when the core comes into contact with water are to be treated. To keep calculations simple, the codes make significant approximations; they neglect the heat of deposited fission products, they assume that aerosols are

well mixed when they may not be, and they treat boundary layer phenomena simplistically.[23]

Many details of how an accident proceeds are very sensitive to parameters that are poorly known or modeled. This problem is even more true of the ultimate consequences. As such, there are probably large but still unknown uncertainties in the present codes. Nevertheless, code development is useful because the codes could provide a measure of understanding of complicated phenomena that is difficult to obtain otherwise.

The Advisory Committee on Reactor Safeguards "conclude[s] that the codes, in their present form, should not be given much weight in making decisions."[24] What is now needed in order to improve understanding is to test these codes—that is, validate them by comparing their predictions with many large-scale, as well as small-scale, experiments. In this way, it would be possible to learn the present uncertainties of the codes and to discover important phenomena that may have been missed. New and improved codes can then be developed in parallel with further experiments. This kind of evolution is now in progress; the NRC is developing new codes, and several large-scale experiments are underway (at Sandia National Laboratories, Idaho National Engineering Laboratory, MARVIKEN, Karlsruhe, and others). There has even been a test of blowdown in a full-scale reactor.

Reliable and versatile codes could be used to predict the consequences of, or even strategies for mitigating, severe accidents with unusual sequences, such as those a terrorist attack might initiate. This kind of understanding of reactor accidents is many years in the future.

Notes

1. M. Silberberg et al., "Reassessment of the Technical Bases for Estimating Source Terms," draft report NUREG-0956 (Washington, D.C.: Nuclear Regulatory Commission, July 1985) (hereafter cited as NUREG-0956).

2. R. Wilson et al., "Report to the American Physical Society of the Study Group on Radionuclide Release from Severe Accidents at Nuclear Power Plants," *Reviews of Modern Physics* 57 (July 1985): S1–S154.

3. American Nuclear Society, "Report of the Special Committee on Source Terms" (LaGrange Park, Ill.: The Society, September 1984); IDCOR Technical Summary Report, "Nuclear Power Plant Response to Severe Accidents" (Atomic Industrial Forum, Inc., Bethesda, Md., November 1984).

4. NUREG-0956.

5. Other sources of up-to-date information on light water nuclear reactor safety and accidents are the annual meetings on this subject organized by the NRC, held in Gaithersburg, Maryland. These meetings, attended by members of the international nuclear safety engineering community, consist of presentations and discussions of research and development plans, results, and conclusions. I suggest that a good way to improve understanding of the terrorist threat to nuclear reactors would be to hold sessions on this problem specifically at these annual meetings, as well as at meetings of the APS and the American Nuclear Society.

6. Advisory Committee on Reactor Safeguards, "Comments on NUREG-0956" (Washington, D.C.: Nuclear Regulatory Commission, December 1985).

7. This point is made in all the reports cited here.

8. NUREG-0956.

9. Wilson et al., "Report."

10. NUREG-0956.

11. American Nuclear Society, "Report."

12. Ibid.

13. Ibid.

14. Advisory Committee on Reactor Safeguards, "Comments."

15. NUREG-0956; American Nuclear Society, "Report."

16. NUREG-0956; American Physical Society, "Report."

17. American Physical Society, "Report."

18. NUREG-0956; American Physical Society, "Report"; American Nuclear Society, "Report."

19. NUREG-0956; IDCOR, "Nuclear Power Plant Response."

20. Advisory Committee on Reactor Safeguards, "Comments."

21. NUREG-0956.

22. American Physical Society, "Report"; Advisory Committee on Reactor Safeguards, "Comments."

23. Ibid.; American Physical Society, "Report"; American Nuclear Society, "Report."

24. Advisory Committee on Reactor Safeguards, "Comments."