



The Design-Basis Threat (U)

An Interagency Security Committee Report

April 12, 2010

Unclassified

For Official Use Only (FOUO)



Cover Photo: The Department of Homeland Security (DHS) state-of-the-art National Operations Center (NOC) serves as the primary, national-level nerve center for real-time threat monitoring, domestic incident management, and vertical and horizontal information sharing efforts. Operating 24 hours a day, seven days a week, 365 days a year, the NOC provides situational awareness and monitoring of the homeland, coordinates incidents and response activities, and issues advisories and bulletins to homeland security partners as well as specific protective and countermeasure guidance. Accommodating more than 35 agency representatives ranging from law enforcement organizations to Federal departments, the NOC serves as a clearinghouse for vital information to determine possibilities of risk or terrorist nexus and shares that information with appropriate officials to strengthen and coordinate security operations where necessary.

Photo from the DHS Photo File



Preface



Todd M. Keil
Assistant Secretary for
Infrastructure Protection

Protecting Federal employees and the public who visit U.S. government-owned or leased facilities from all hazards is a complex and challenging responsibility. It is also one of our top national priorities and the mission of the Interagency Security Committee (ISC).

As Chair of the ISC, I am pleased to introduce a new interim ISC Report, titled *The Design-Basis Threat (DBT)*, which is to be used during a 24-month validation period. This validation period will allow user input to inform the final report.

The DBT Report is a stand-alone threat analysis to be used with the *Physical Security Criteria for Federal Facilities: An ISC Standard*. The document establishes a profile of the type, composition, and capabilities of adversaries, and it is also designed to correlate with the countermeasures in the compendium of standards and to be easily updated as needed.

The DBT is an estimate of the threats that face Federal facilities across a range of undesirable events and based on the best intelligence information, Intelligence Community (IC) reports and assessments, and crime statistics available to the working group at the time of publication. Users of the DBT must consider that undiscovered plots may exist, adversaries are always searching for new methods and tactics to overcome security measures, and the lone-wolf adversary remains largely unpredictable.

The intent of the DBT is threefold:

- To inform the deliberations of ISC working groups as they establish standards;
- To support the calculation of risk, based upon threat, vulnerability, and consequences, to a facility, when applying ISC's *Physical Security Criteria for Federal Facilities*; and
- To determine specific adversary characteristics that performance standards and countermeasures are designed to overcome.

The validation period over the next 24 months will clarify any needed changes or updates to the overall usability of the Report. As threats change and events occur, the report will be updated on a six month basis.

The report is another significant milestone and represents exemplary collaboration across the entire ISC. I want to especially commend the members of the DBT working group for all the hard work they put into the development of this report.

Todd M. Keil
Assistant Secretary for Infrastructure Protection

Interagency Security Committee Participants

ISC Chair

Todd Keil

Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

ISC Executive Director

Austin L. Smith
Office of Infrastructure Protection
U.S. Department of Homeland Security

Working Group Chair

Thomas Wood
Chief, Physical Security Branch
Building Security and Policy Division
Public Buildings Service
U.S. General Services Administration

Working Group Members

Bobby Deitch
Physical Security Specialist
Building Security and Policy Division
Public Buildings Service
U.S. General Services Administration

Michael Griffin
Physical Security Specialist
Building Security and Policy Division
Public Buildings Service
U.S. General Services Administration

Thomas Magee
Physical Security Specialist
Security Division – Heartland Region
Public Buildings Service
U.S. General Services Administration

Gary R. Riden
Regional Coordinator for the Middle East,
Physical Security Division, Diplomatic
Security Service
U.S. Department of State

Joseph A. Zaranka
Chief, Facilities Security Division
Office of Physical Security Programs
Bureau of Diplomatic Security
U.S. Department of State

Michael Fritz
Chief, Domestic Buildings Branch
Facilities Security Division
Bureau of Diplomatic Security
U.S. Department of State

Bernard Holt
Senior Policy Analyst
Interagency Security Committee
Office of Infrastructure Protection
U.S. Department of Homeland Security

J. Patrick Nash
Program Manager
Force/Executive Protection
Security Division
Federal Bureau of Investigation

Shawn Turonis
Supervisory Special Agent
Federal Protective Service
National Protection and Programs Directorate
U.S. Department of Homeland Security

The working group also extends its thanks to the men and women of the intelligence and law enforcement communities, whose collection and analytical support directly aided this effort, and whose tireless efforts help to safeguard the United States from all enemies, foreign and domestic.

“Today we were unlucky, but remember we only have to be lucky once. You will have to be lucky always.”

- Communiqué from the Irish Republican Army to British Prime Minister Margaret Thatcher, on the occasion of the bombing of the Grand Hotel in Brighton, England, October 12, 1984

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or personnel who do not have a valid “need-to-know” without prior approval of the authorized DHS official.

At a minimum, this document will be disseminated only on a need-to-know basis, and when unattended, will be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

When no longer needed, destroy this material by shredding, pulping, or burning to assure destruction beyond recognition.

Contents

1.0	<u>Background</u>	1
2.0	<u>Applicability and Scope</u>	2
3.0	<u>Document Control</u>	3
4.0	<u>Definitions (Listed by Relationship to Each Other)</u>	4
5.0	<u>How to Apply This Report</u>	5
5.1	ISC Working Groups	5
5.2	Risk Assessment	5
5.3	Performance Standards	6
5.4	Updates	6
6.0	<u>Threat Assessment of Undesirable Events</u>	7
6.1	Administrative Information	8
6.2	Definitions	8
6.3	Design-Basis threat Scenarios	8
6.4	Baseline Threats	8
6.5	Analytical Basis	9
6.6	Target Attractiveness	10
6.7	Outlook	10
6.8	References	10
6.9	Acronyms and Definitions	11
7.0	<u>Undesirable Events (To be Placed in Separate Sections of a Notebook)</u>	13
7.1	<u>Aircraft as a Weapon</u>	7.1.1
	Design-Basis Threat Scenario	7.1.1
	Baseline Threat	7.1.1
	Analytical Basis	7.1.1
	Target Attractiveness	7.1.3
	Outlook	7.1.4
7.2	<u>Arson</u>	7.2.1
	Design-Basis threat Scenario	7.2.1
	Baseline Threat	7.2.1
	Analytical Basis	7.2.1
	Target Attractiveness	7.2.2
	Outlook	7.2.3
7.3	<u>Assault</u>	7.3.1
	Design-Basis Threat Scenario	7.3.1
	Baseline Threat	7.3.1
	Analytical Basis	7.3.1
	Target Attractiveness	7.3.2

	Outlook	7.3.3
7.4	<u>Ballistic Attack – Active Shooter</u>	7.4.1
	Design-Basis Threat Scenario	7.4.1
	Baseline Threat	7.4.1
	Analytical Basis	7.4.1
	Target Attractiveness	7.4.3
	Outlook	7.4.3
7.5	<u>Ballistic Attack – Small Arms</u>	7.5.1
	Design-Basis Threat Scenario	7.5.1
	Baseline Threat	7.5.1
	Analytical Basis	7.5.1
	Target Attractiveness	7.5.2
	Outlook	7.5.2
7.6	<u>Ballistic Attack – Standoff Weapons</u>	7.6.1
	Design-Basis Threat Scenario	7.6.1
	Baseline Threat	7.6.1
	Analytical Basis	7.6.1
	Target Attractiveness	7.6.3
	Outlook	7.6.3
7.7	<u>Breach of Access Control Point – Covert</u>	7.7.1
	Design-Basis Threat Scenario	7.7.1
	Baseline Threat	7.7.1
	Analytical Basis	7.7.1
	Target Attractiveness	7.7.2
	Outlook	7.7.2
7.8	<u>Breach of Access Control Point – Overt</u>	7.8.1
	Design-Basis Threat Scenario	7.8.1
	Baseline Threat	7.8.1
	Analytical Basis	7.8.1
	Target Attractiveness	7.8.1
	Outlook	7.8.2
7.9	<u>CBR Release –External</u>	7.9.1
	Design-Basis Threat Scenario	7.9.1
	Baseline Threat	7.9.1
	Analytical Basis	7.9.1
	Target Attractiveness	7.9.2
	Outlook	7.9.3

7.10	<u>CBR Release – Internal</u>	7.10.1
	Design-Basis Threat Scenario	7.10.1
	Baseline Threat	7.10.1
	Analytical Basis	7.10.1
	Target Attractiveness	7.10.2
	Outlook	7.10.3
7.11	<u>CBR Release – Mailed or Delivered</u>	7.11.1
	Design-Basis Threat Scenario	7.11.1
	Baseline Threat	7.11.1
	Analytical Basis	7.11.1
	Target Attractiveness	7.11.3
	Outlook	7.11.3
7.12	<u>CBR Release – Water – Supply</u>	7.12.1
	Design-Basis Threat Scenario	7.12.1
	Baseline Threat	7.12.1
	Analytical Basis	7.12.1
	Target Attractiveness	7.12.3
	Outlook	7.12.3
7.13	<u>Civil Disturbance</u>	7.13.1
	Design-Basis Threat Scenario	7.13.1
	Baseline Threat	7.13.1
	Analytical Basis	7.13.1
	Target Attractiveness	7.13.2
	Outlook	7.13.2
7.14	<u>Coordinated or Sequential Attack</u>	7.14.1
	Design-Basis Threat Scenario	7.14.1
	Baseline Threat	7.14.1
	Analytical Basis	7.14.1
	Target Attractiveness	7.14.2
	Outlook	7.14.3
7.15	<u>Disruption of Building or Security Systems</u>	7.15.1
	Design-Basis Threat Scenario	7.15.1
	Baseline Threat	7.15.1
	Analytical Basis	7.15.1
	Target Attractiveness	7.15.1
	Outlook	7.15.2
7.16	<u>Explosive Device – Mailed or Delivered</u>	7.16.1
	Design-Basis Threat Scenario	7.16.1

	Baseline Threat	7.16.1
	Analytical Basis	7.16.1
	Target Attractiveness	7.16.3
	Outlook	7.16.4
7.17	<u>Explosive Device – Man-Portable External</u>	7.17.1
	Design-Basis Threat Scenario	7.17.1
	Baseline Threat	7.17.1
	Analytical Basis	7.17.1
	Target Attractiveness	7.17.3
	Outlook	7.17.4
7.18	<u>Explosive Device – Man-Portable Internal</u>	7.18.1
	Design-Basis Threat Scenario	7.18.1
	Baseline Threat	7.18.1
	Analytical Basis	7.18.1
	Target Attractiveness	7.18.3
	Outlook	7.18.4
7.19	<u>Explosive Device – Suicide or Homicide Bomber</u>	7.19.1
	Design-Basis Threat Scenario	7.19.1
	Baseline Threat	7.19.1
	Analytical Basis	7.19.1
	Target Attractiveness	7.19.3
	Outlook	7.19.4
7.20	<u>Explosive Device – Vehicle Borne IED</u>	7.20.1
	Design-Basis Threat Scenario	7.20.1
	Baseline Threat	7.20.1
	Analytical Basis	7.20.1
	Target Attractiveness	7.20.8
	Outlook	7.20.9
7.21	<u>Hostile Surveillance</u>	7.21.1
	Design-Basis Threat Scenario	7.21.1
	Baseline Threat	7.21.1
	Analytical Basis	7.21.1
	Target Attractiveness	7.21.3
	Outlook	7.21.3
7.22	<u>Insider Threat</u>	7.22.1
	Design-Basis Threat Scenario	7.22.1
	Baseline Threat	7.22.1
	Analytical Basis	7.22.1

	Target Attractiveness	7.22.2
	Outlook	7.22.2
7.23	<u>Kidnapping</u>	7.23.1
	Design-Basis Threat Scenario	7.23.1
	Baseline Threat	7.23.1
	Analytical Basis	7.23.1
	Target Attractiveness	7.23.3
	Outlook	7.23.3
7.24	<u>Release of Onsite Hazardous Materials</u>	7.24.1
	Design-Basis Threat Scenario	7.24.1
	Baseline Threat	7.24.1
	Analytical Basis	7.24.1
	Target Attractiveness	7.24.2
	Outlook	7.24.2
7.25	<u>Robbery</u>	7.25.1
	Design-Basis Threat Scenario	7.25.1
	Baseline Threat	7.25.1
	Analytical Basis	7.25.1
	Target Attractiveness	7.25.2
	Outlook	7.25.2
7.26	<u>Theft</u>	7.26.1
	Design-Basis Threat Scenario	7.26.1
	Baseline Threat	7.26.1
	Analytical Basis	7.26.1
	Target Attractiveness	7.26.2
	Outlook	7.26.2
7.27	<u>Unauthorized Entry – Forced</u>	7.27.1
	Design-Basis Threat Scenario	7.27.1
	Baseline Threat	7.27.1
	Analytical Basis	7.27.1
	Target Attractiveness	7.27.2
	Outlook	7.27.3
7.28	<u>Unauthorized Entry – Surreptitious</u>	7.28.1
	Design-Basis Threat Scenario	7.28.1
	Baseline Threat	7.28.1
	Analytical Basis	7.28.1
	Target Attractiveness	7.28.2
	Outlook	7.28.3

7.29	<u>Vandalism</u>	7.29.1
	Design-Basis Threat Scenario	7.29.1
	Baseline Threat	7.29.1
	Analytical Basis	7.29.1
	Target Attractiveness	7.29.2
	Outlook	7.29.2
7.30	<u>Vehicle Ramming</u>	7.30.1
	Design-Basis Threat Scenario	7.30.1
	Baseline Threat	7.30.1
	Analytical Basis	7.30.1
	Target Attractiveness	7.30.2
	Outlook	7.30.2
7.31	<u>Workplace Violence</u>	7.31.1
	Design-Basis Threat Scenario	7.31.1
	Baseline Threat	7.31.1
	Analytical Basis	7.31.1
	Target Attractiveness	7.31.3
	Outlook	7.31.3
7.32	<u>References for Undesirable Events</u>	7.32.1

1.0 Background

In 2006, the Interagency Security Committee (ISC) membership established a working group to update, expand, and clarify all security standards for protecting Federal facilities, and publish them in one compendium. The first product of the working group, “Facility Security Level Determinations for Federal Facilities” was released in March of 2008.

As the working group began work on its second document, “Physical Security Criteria for Federal Facilities,” it was recognized that the threat to Federal facilities had to be addressed differently for a variety of reasons. First, the threat was typically based on publicized historical events, leading the government to design tomorrow’s facilities to meet yesterday’s threats. Today’s dynamic threat environment suggests a need to react to rapid change. The elapsed time between the identification of a need for a new Federal facility and the time it is occupied can be as long as 7 to 10 years. In that time, the threat has likely changed substantially. Previous standards also incorporated aspects of the threat as part of the document itself, which made it difficult to keep the threat current without updating the entire standard. The threat changes faster than working groups can develop new standards.

Additionally, while the nature of the criminal and terrorist threat to Federal facilities has changed substantially, the desired effectiveness of our protective measures remains fairly static. For example, while the size and makeup of a potential improvised explosive device (IED) may increase as terrorist capabilities change over time, the desired performance of the windows to an IED (e.g., limit fragmentation to within 10 feet of the window) usually remains the same.

Further, the validity of the threat is routinely called into question, not only in the characteristics of the threat itself (e.g., device size, weapon caliber, sophistication of the adversary, etc.), but in its applicability to a specific facility. More information was needed to support the evaluation of the threat as it pertains to the estimation of risk for each facility. By providing guidance in that area, the consistency of threat ratings from facility to facility is improved.

The ISC Standards Subcommittee, charged with ensuring consistency among the various standards, also recognized that the methodology of incorporating the threat into the standards development process was inadequate and inconsistent. Previous documents developed the threat based solely on the knowledge of working group participants, without necessarily the expertise in or availability of intelligence analysis. In some cases, the threat was not determined based on intelligence or trends, but by how much government agencies felt they could afford to spend, or what facilities could be built to withstand. This did not provide a complete understanding of the risks posed to Federal facilities; rather, it represented the level of risk the developers felt could be addressed at the time. By providing a true estimate of the threat as the basis for design and development

of new standards, it is possible to know if risk is being accepted when funding or technology is not available to meet what is estimated to be the true threat. This understanding of risk is crucial to a sound risk-based approach to securing Federal facilities.

Finally, with multiple working groups developing and updating a variety of related standards, the need for consistent information regarding the threat to serve as the basis for all new standards is paramount. Each working group should be considering the same threat as they write standards to counter it. For example, in establishing standards for ballistic resistance of protective vests, a working group developing standards for contract guards should be considering the same weapons as a working group considering ballistic protection around a screening area. As updates become necessary, having an understanding of the nature and level of threat considered in the development of an old standard will aid in identifying areas where updates are necessary to meet changing conditions.

Thus, a working group was formed to develop a standalone threat document to be included in the compendium. “The Design-Basis Threat” (DBT) is the result. The DBT establishes a profile of the type, composition, and capabilities of adversaries. In order to ensure the validity, ISC members with experience in developing and analyzing threat information, and with access to the most current intelligence available, were selected to participate in the development. The design of the document is such that it can be updated easily, and correlated with the countermeasures in “Physical Security Criteria for Federal Facilities.”

2.0 Applicability and Scope

This report is issued pursuant to the authority of the Interagency Security Committee (ISC) contained in Executive Order 12977, October 19, 1995, "Interagency Security Committee", as amended by Executive Order 13286, March 5, 2003.

This report is applicable generically to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. Management officials, security organizations, and ISC working groups should reference the most current edition of “The Design-Basis Threat,” (DBT) unless a current agency-specific threat assessment publication addressing the undesirable events is available.

The events addressed in this document are man-made. Natural hazards such as earthquakes, floods, fire, or wind storms are beyond the scope of this document and addressed in applicable construction and life safety standards. For further information on the threat of and strategies to mitigate natural hazards, please visit the Federal Emergency Management Agency (FEMA) website at www.fema.gov. Additionally, this document does not address the cyber threat to Federal facilities. For further information on the cyber threat and mitigation strategies, please visit

“It is important to change the methods of attacks and strikes...”

—Sheikh Ayman al-Zawahiri

the U.S. Computer Emergency Readiness Team (US-CERT) website at www.us-cert.gov.

The DBT is an *estimate* of the threat that faces Federal facilities across a range of undesirable events and based on the best intelligence information, Intelligence Community (IC) reports and assessments, and crime statistics available to the working group at the time of publication. However, users of the DBT must consider that undiscovered plots may exist, adversaries are always searching for new methods and tactics to overcome security measures, and the lone-wolf adversary remains largely unpredictable.

3.0 Document Control

This report is Unclassified – For Official Use Only (FOUO) and should be released only to those with a need-to-know. In the past it has been common practice to provide design consultants or realty brokerage firms with a complete copy of a standards document. This practice provides them more information than required to complete their work and is not permitted.

Specific security requirements – expressed in performance terms where possible – are to be developed by the government based on the Design-Basis Threat (DBT) and provided to design consultants. In this manner, only the information required will be released outside of the government, and information that is outside the scope of a project will not be released to persons without a valid need-to-know. For example, while the DBT device size for an Improvised Explosive Device) may be provided to a design team, the information upon which that device size was predicated should not be released.

All specific security requirements and design documents developed in accordance with this report must be marked as For Official Use Only or higher as appropriate, and protected accordingly.

A classified annex addressing specific undesirable events has been developed to provide more detail as appropriate. If the classified annex is applicable to a particular event, it is noted in the administrative header block of the individual DBT event. Users requiring access to the classified annex should visit the Interagency Security Committee website at www.dhs.gov/isc for availability and to coordinate the transmission of a copy.

4.0 Definitions (Listed by relationship to each other)

For the purposes of this report, the following definitions apply. For ease of comparison, the definitions are grouped according to relationship to each other. An alphabetized list of definitions and acronyms is also provided on page 12.

Design-Basis Threat (DBT): A profile of the type, composition, capabilities, methods (tactics, techniques, and procedures), and motivation of an adversary upon which the security engineering and operations of a facility is based.

Baseline Threat: The estimate of the relative threat posed to a Federal facility from an Undesirable Event and categorized as Very Low, Low, Moderate, High or Very High.

Undesirable Event: An incident that has an adverse impact on the operation of the facility or mission of the agency.

Level of Protection (LOP): The degree of security provided by a particular countermeasure or set of countermeasures. Levels of Protection used in this Standard are Minimum, Low, Moderate, High, and Very High.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified undesirable event.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Threat: The intention and capability of an adversary to initiate an undesirable event.

Vulnerability: A weakness in the design or operation of a facility that can be exploited by an adversary.

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

5.0 How to Apply This Report

The Design-Basis Threat (DBT) establishes the characteristics of the threat environment to be used in conjunction with Interagency Security Committee physical security standards.

The intent of the DBT is three-fold:

- To inform the deliberations of ISC working groups as they establish standards;
- To support the calculation of the threat, vulnerability, and consequence to a facility when calculating risk to a Federal facility and determining an appropriate Level of Protection, particularly when applying ISC's "Physical Security Criteria for Federal Facilities;" and,
- To determine specific adversary characteristics that performance standards and countermeasures are designed to overcome.

5.1 *ISC Working Groups*

It is critical that as ISC working groups develop standards to address threats against Federal facilities, they have a clear understanding of the threat they are trying to counter. ISC working groups should use the ISC DBT as the basis for quantifying and characterizing threats in general. Standards should be commensurate with the threats presented in the DBT.

For example, requirements for guard force training, equipment, and weapons should be based on the DBT's postulated adversary capabilities for such events are robbery, assault, workplace violence, ballistic attacks, etc. In the case of graduated standards, such as those provided by the ISC's "Physical Security Criteria for Federal Facilities," increasing levels of protection should be based on descriptions of factors that heighten the threat or increase the intensity of the event for higher-risk facilities.

5.2 *Risk Assessments*

The DBT provides specific details as to the characteristics of each event that might take place at a Federal facility. They are based on a worst-reasonable-case. Each event provides sufficient information from which the threat, consequences, and vulnerability can be estimated in the conduct of a risk assessment:

- A baseline threat rating is provided, and target attractiveness characteristics which may make a facility more attractive as a target (increase the threat) are enumerated as appropriate. These factors should be considered in determining a score or rating for "threat." Deviation

from this threat level should be fully documented and supported with current intelligence information.

- The specifics about the size, number, equipment, etc. included in the scenario can be used to estimate the potential consequences. Consequence estimates should be based on the potential effects of a successful undesirable event.
- The specifics of the scenario should also be used to measure the effectiveness of existing protective measures in determining vulnerability. The vulnerability score should reflect the likelihood of the existing countermeasure successfully resisting or overcoming the DBT event scenario

Where appropriate, modifications to the event scenarios are permitted. However, modifications must be supported with a detailed rationale, and should provide sufficient detail to support the quantification of threat, consequence, and vulnerability.

Additionally, in estimating the threat level, specific information unique to the facility or the locale may be used. Local crime statistics, the tactics of adversary groups known to be operating in a particular area, and other actionable intelligence that suggests a different threat level may modify the threat from the baseline. When used, this information must be fully documented.

5.3 Performance Standards

In designing countermeasures to defeat or mitigate specific events, the characteristics of the DBT event scenarios should be considered as design parameters for performance of a countermeasure. For example, when it is necessary to protect a facility against a vehicle-borne improvised explosive device (VBIED), the device size specified for VBIED events should be used for engineering calculations.

5.4 Updates

In order to keep pace with the changing nature of the threat to Federal facilities, updates to the DBT will be made periodically. Users of this document should visit the ISC website at www.dhs.gov/isc for relevant information that may affect this and other ISC documents affecting the security of Federal facilities.

ISC standard operating procedures will dictate a time-span for routine updates of the entire document. When conditions or events suggest a change to the threat environment relating to one or more undesirable events, updates will be made for specific events. The document was structured with this thought in mind: a single

undesirable event can be updated and distributed to the community without the need for a complete rewrite (and subsequent review period) of the entire report.

Similarly, if users of the document become aware of information which may serve as further examples of the DBT or which may impact the assessed threat, they are asked to notify the ISC so that new information may be included and the document remains as up-to-date and accurate as possible.

6.0 Threat Assessment of Undesirable Events

Each event is presented as a standalone document. As the need arises, event documents may be updated or replaced, and undesirable events added in order to keep this report as current as possible.

Analysis and synthesis of the threat stream – and in particular the consolidation of threat reporting from various members of the intelligence community (IC) – has been an ongoing effort since the creation of the U.S. Department of Homeland Security (DHS). Volumes of applicable information already exist in disparate reports from a variety of agencies. This document is an extension of that goal of consolidation. Where sufficient information was already collected, quality analysis conducted, or applicable reports were already prepared, that information was to be consolidated into this document. In some cases, further analysis may have been necessary to make the information more clearly applicable to the protection of Federal facilities, or to more clearly define the characteristics of an event.

In conducting this assessment, the Working Group adhered to the specifications of the 2009 DHS National Infrastructure Protection Plan (NIPP) for conducting a threat assessment:

- Broad spectrums of attack methods that may be employed have been identified.
- In identifying target attractiveness factors, each event document accounts for an adversary's ability to recognize the target.
- In assessing events where security measures outside the influence of Federal facilities impact the planning and implementation by adversaries, the deterrence value of those existing security measures is considered. (Deterrence of on-site countermeasures is considered in determining vulnerability as part of a facility-specific-risk assessment.)
- The level of demonstrated capabilities of adversaries with regard to each particular attack method is considered.

- The degree of the adversaries' intent to carry out such attacks against Federal facilities is considered.
- The likelihood that an adversary would attempt a given attack method against a Federal facility has been estimated.

Each undesirable event document is presented in a standard format. The following describes the contents of each section.

6.1 Administrative Information

A header block contains administrative information regarding the event, including:

- Title of the event
- The original assessment date, which identifies when the event was first considered, analyzed, and included in the DBT report
- The revision number and date of the event document. Revision "0" is the original assessment.
- Indication of whether a classified annex exists, and if so, the classification level and the date of the classified annex

6.2 Definition

A definition of the event is provided to ensure a common understanding of the threat act being considered. The definition is a standardized means of categorizing the event and the types of activities which are addressed by the event, and is not intended as the legal definition.

6.3 Design-Basis Threat Scenario

The design-basis threat scenario provides specific characteristics of the event, such as numbers of adversaries, sizes, speeds, tactics, etc. These details provide the information needed to develop performance specifications to evaluate and design countermeasures for the specific threat, as well as provide a basis for determining potential consequences.

Due to the variety of Federal facilities, in some cases two different scenarios are presented (e.g., a specific scenario applicable to facilities with child care centers, as well as a scenario which is applicable to all facilities).

Due to the different types of variants associated with a particular Undesirable Event, in some cases two different scenarios are presented to provide alternatives.

6.4 Baseline Threat

An estimate of the relative threat posed to Federal facilities is provided, along with a summary of the rationale for the level. Ratings include **VERY LOW, LOW, MODERATE, HIGH, or VERY HIGH**. The base line threat levels are estimates based on an analysis of the United States Department of State's design basis threat (DBT) mathematical model using Expert Choice software, the work groups DBT mathematical model, and taking into account major undesirable events that occur more frequently overseas than in the continental United States. The following factors were used in the assessment:

- Complexity of the event
- Availability of materials necessary for the event
- The prevalence of adversaries willing to carry out the act
- The level of ideology or willingness associated with the event
- Planning and organizational capabilities
- The assessed level of intent of adversaries to carry out the act
- The frequency of historic events
- The involvement of Federal facilities in historic events

The baseline threat level is intended to address Federal facilities generically. When being used by working groups to develop national or broad standards, the baseline threat level is applicable.

When being used to determine threat scores for a specific facility, users are expected to tailor the threat level based on known threat information applicable to the specific facility such as local crime rates, historical events at the facility, or known adversary organizations operating in the vicinity. Absent information which merits a modification, the baseline threat level is applicable. Factors which may modify the baseline threat level are identified in the Target Attractiveness section (see 6.6, below). Whenever the threat level is determined to deviate from the baseline provided here, the factors which influenced the rating must be documented and fully supported by detailed information as part of the assessment.

6.5 Analytical Basis

The analytical basis upon which the DBT scenario baseline threat, target attractiveness considerations, and outlook are predicated, where applicable, examples of incidents are provided to demonstrate the historical basis and capability of adversaries, and to show possible variations on the design-basis threat scenario.

The analytical basis section is by no means all-inclusive of the information which was considered in estimating the threat. Rather, it is a synopsis of the most relevant information.

6.6 *Target Attractiveness*

Target attractiveness considerations are provided to aid in identifying aspects of a particular facility that may make it more or less likely to be a target of a particular undesirable event, subsequently modifying the baseline threat to the facility.

Additionally, when applicable, factors are identified which may change the parameters of the event, such as indicating potential use of a larger explosive device, more adversaries, or more complex methods of attack.

In assessing a specific facility, users are expected to consider target attractiveness factors and modify the threat rating as appropriately. A facility which embodies greater target attractiveness may face a higher threat. Whenever the threat level is determined to deviate from the baseline, the target attractiveness factors which influenced the rating must be documented and fully supported by detailed information as part of the assessment.

Users may wish to apply a specific methodology to determining target attractiveness, such as the U.S. Department of Defense's Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability (CARVER) method, or Sandia's Risk Assessment Methodology (RAM) approach, which has been customized to fit a variety of infrastructure.

6.7 *Outlook*

In many cases, the assessment-budgeting-implementation cycle (and the standards-development cycle) is lengthy and may exceed the value of current threat information. In order to support long-range planning and design-construction efforts, an outlook section is provided to describe what is assessed to be the changes in the threat over time.

6.8 *References*

References to supporting information and source reports are provided as applicable.

6.9 Acronyms and Definitions

Acronyms

CBR	Chemical-Biological-Radiological
CBRN	Chemical-Biological-Radiological-Nuclear
CBRNE	Chemical-Biological-Radiological-Nuclear and High-Yield Explosive
DBT	Design Basis Threat
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GAO	Government Accountability Office
GSA	General Services Administration
HMTD	Hexamethylene Triperoxide Diamine
IC	Intelligence Community
IID	Improvised Incendiary Device
IED	Improvised Explosive Device
ISC	Interagency Security Committee
LAAW	Light Anti-Armor Weapon
LOP	Level of Protection
NOC	National Operations Center (DHS)
RPG	Rocket-Propelled Grenade
TATP	Triacetone Triperoxide
US-CERT	United States Computer Emergency Readiness Team
VBIED	Vehicle-Borne Improvised Explosive Device

Definitions (Listed alphabetically)

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

Design-Basis Threat (DBT): A profile of the type, composition, capabilities, methods (tactics, techniques, and procedures), and motivation of an adversary upon which the security engineering and operations of a facility is based.

Level of Protection (LOP): The degree of security provided by a particular countermeasure. Levels of Protection used in this Standard are Minimum, Low, Moderate, High, and Very High.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified undesirable event.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Threat: The intention and capability of an adversary to initiate an undesirable event.

Undesirable Event: An incident that has an adverse impact on the operation of the facility or mission of the agency.

Vulnerability: A weakness in the design or operation of a facility that can be exploited by an adversary.

7.0 Undesirable Events

This section lists some undesirable events that could have an adverse impact on the operation of a facility or mission of a Federal agency.

Aircraft as a Weapon	Attack on a facility using an aircraft as an improvised explosive device.
Arson	Accessing a facility and deliberately setting fire to the facility or to assets within the facility.
Assault	Physically assaulting (with or without a weapon) a person or persons inside the facility or on the property.
Ballistic Attack - Active Shooter	An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms.
Ballistic Attack - Small Arms	Firearm fired from offsite into a facility or a defined area.
Ballistic Attack - Standoff Weapons	Mortar, rocket-propelled grenade, etc., fired from offsite into a facility or area.
Breach of Access Control Point - Covert	Use of deceit, coercion, or social engineering to gain access to a facility through a controlled entrance.
Breach of Access Control Point - Overt	The use of force and/or weapons to defeat a personnel screening or access control checkpoint (including ID checks).
Chemical/Biological/Radiological Release - External	Intentional release of a CBR agent into a facility through a specific access point, such as; air intake, windows, or doorways, from outside the facility.
CBR Release - Internal	Intentional release of a CBR agent carried into the facility, including in general interior spaces (lobbies) or into specific rooms or systems (HVAC rooms).
CBR Release - Mailed or Delivered	A CBR substance or dispersal device sent to the facility through US Mail or a commercial delivery service, including an unwitting courier.
CBR Release - Water Supply	Intentional release of a CBR agent into a facility's potable water supply, from a location outside the facility.
Civil Disturbance	Deliberate and planned acts of violence and destruction stemming from organized demonstrations on or near Federal property.
Coordinated or Sequential Attack	A planned assault on a facility that integrates the aspects of several undesirable events.
Disruption of Building & Security Systems	Physically accessing building or security systems for the purposes of disruption or manipulation of the systems.
Explosive Device-Mailed or Delivered	An explosive device sent to the facility through U.S. Mail or a commercial delivery service, including an unknowing courier.
Explosive Device - Man-Portable External	An explosive device placed on the property, outside of a building and left to detonate after the adversary departs.
Explosive Device - Man-Portable Internal	An explosive device carried into the building by an adversary or an unsuspecting occupant, visitor, or courier, and left to detonate after the adversary departs.
Explosive Device - Suicide/Homicide Bomber	An explosive device carried into the building by an adversary with the intent of reaching a specific target or area then detonating, killing or injuring the bomber and others.
Explosive Device - VBIED	An attack against a facility that utilizes a vehicle to deliver an improvised explosive device.
Hostile Surveillance	The surveillance of key assets, personnel, security features, operations, or sensitive areas from offsite, or outside secure areas for the purposes of collection of information in preparation for an attack.
Insider Threat	Individuals with the access and/or inside knowledge of an organization that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.
Kidnapping	Abduction of an occupant or visitor from a facility, including from inside secured areas (e.g., a child care center) or outside on the site (e.g., a Government-controlled parking lot).
Release of Onsite Hazardous Materials	Unauthorized access to hazardous materials stored onsite with the intent of harming personnel or damaging the facility.
Robbery	Unauthorized taking of Government-owned or personal property from an employee or other person(s) by force or threat of force. The incident could occur inside or outside of a facility.
Theft	Unauthorized removal of Government-owned or personal property from a facility.
Unauthorized Entry - Forced	Unauthorized access to a facility or controlled area by forced entry.
Unauthorized Entry - Surreptitious	Unauthorized access to a facility or controlled area by stealth.
Vandalism	Destruction, damage, or defacing of Government-owned or personal property or assets.
Vehicle Ramming	Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock) or breach a defined perimeter.
Workplace Violence	Violence perpetrated by an authorized occupant or an employee. The assailant can be another employee, authorized tenant, or an authorized visitor.

Undesirable Event	7.1 Aircraft as a Weapon					
Definition	Attack on a facility using an aircraft as an improvised explosive device.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Deliberately crashing a Cessna 172 Skyhawkⁱ (or similar) into a facility. The Cessna 172's characteristics are as follows:

- Maximum cruise speed: 126 knots (233 km/h)
- Max takeoff weight: 2550 lbs (1157 kg)
- Useable fuel capacity: 318 lbs (144 kg)
- Full fuel payload: 523 lbs (237 kg)
- Range: 610 nm (1130 km)
- Height: 8 ft 11 in (2.72 m)
- Length: 27 ft 2 in (8.28 m)
- Wingspan: 36 ft 1 in (11 m)

Baseline Threat

The continuing interest by certain terrorist organizations in this method of attack, disruption of recent plots to commandeer aircraft, and historical frequency, suggests the threat of this event would be high. However, the extensive security measures taken in the commercial aviation security sector to mitigate the threat to aircraft also mitigates the threat to Federal facilities, before it can manifest itself against a facility. Consequently, the baseline threat to Federal facilities from this event is assessed to be **LOW**.

Analytical Basis

Terrorist organizations and lone-wolf adversaries have demonstrated the capability and intent of taking control of aircraft and using them against government facilities for various purposes. Examples of such events include the following:

- On February 18, 2010, Andrew Joseph Stack III flew his Piper Dakota aircraft into the Echelon office complex in Austin Texas, killing himself and Internal Revenue Service manager Vernon Hunter. Thirteen others were injured, two seriously. The Internal Revenue Service (IRS) field office was located in this four-story office building along with other state and federal government agencies.

7.1.1

On the morning of the crash, Stack posted a suicide note on his website. In the suicide note, he expressed displeasure with the government, the bailouts, politicians, General Motors, Enron, Arthur Andersen, the unions, the drug and health care insurance companies, the Catholic Church, the FAA and having a long-running feud with the IRS.ⁱⁱ

- On April 6, 2009, Yavuz Berke, a 31-year-old naturalized Canadian citizen, stole a Cessna 172 from a flight school in Canada and flew the aircraft into the U.S. Berke's intentions were unknown, but he left a suicide note. The state Capitol building in Madison, WI was evacuated during the incident.
- On February 20, 2009, the Tamil Tigers attempted two suicide attacks using Czech-built Morovan Zlin-143 aircraft, loaded with approximately 500 pounds of C-4 explosive. One plane was shot down, while a second struck a tax office in downtown Colombo, Sri Lanka. The explosives did not detonate. The ZUN-143 is similar in dimensions and performance to the Cessna 172.
- On January 5, 2002, 15-year-old Charles J. Bishop deliberately flew a Cessna 172 into the Bank of America tower in Tampa, FL. A note found in the plane stated "Osama bin Laden is absolutely justified in the terror he has caused on 9-11. He has brought a mighty nation to its knees! God blesses him and the others who helped make September 11th happen."
- In 2002, Al-Qa'ida planned a suicide hijacking to attack the U.S. Bank Tower/Library Tower in Los Angeles. Jemaah Islamiya (JI), al-Qa'ida's Southeast Asian terrorist affiliate, was to provide Southeast Asian men as operatives to avoid arousing suspicion. The terrorists were planning to use shoe bombs to gain access to the cockpit.
- On September 11, 2001, al-Qa'ida terrorists seized control of 4 commercial passenger airliners with the intent of deliberately crashing them into iconic targets in the United States. Three aircraft reached their targets: the World Trade Center towers in New York City and the Pentagon outside of Washington, DC. The fourth crashed into a field in Shanksville, PA after passengers attempted to retake control of the aircraft.
- On September 12, 1994, Frank Eugene Corder crashed a stolen Cessna 150 on the lawn just south of the White House, striking a corner of the building. Corder was depressed and on drugs.

Using a general aviation (GA) aircraft requires less planning, sophistication, and coordination that could lead to a plot being discovered by authorities. Flying a GA aircraft requires less flight training than a more advanced commercial aircraft. Law enforcement and intelligence authorities are aware of terrorist organizations obtaining or attempting to obtain flight training, including the use of advanced flight simulation programs. The availability of GA aircraft such as the Cessna 172 makes them a likely weapon. More than 200,000 GA aircraft are based at over 19,000 GA airfields around the U.S.ⁱⁱⁱ

The Cessna 172 Skyhawk is reputed to be the “most popular private aircraft” in the world, with over 43,000 produced and in-service since 1956.^{iv} In the case of Mathias Rust, the aircraft was rented legitimately. Corder, Berke, and Bishop, all of whom had some amount of flight training, stole aircraft from local GA airports.

- In May 2003, reports linked Al-Qa’ida to a plan to fly an explosives-laden general aviation aircraft into the U.S. Consulate in Karachi, Pakistan.

In the short-term, the increased level of security measures for commercial aviation and the challenges associated with overpowering a larger crew (and passengers) makes use of a commercial passenger aircraft more difficult since the 9-11 attacks. However, penetration testing has shown that the security measures are not infallible.

The complexity of fusing an explosive device to detonate upon impact of the aircraft is thought to be such that combining an explosive device into the event is unlikely. Such an attack was attempted by the Tamil Tigers in 2009 but the explosives failed to function. No other successful attempts at incorporating an explosive into the attack have been achieved.

Target Attractiveness

Level V facilities, national monuments and icons, highly symbolic commercial office towers, other highly symbolic facilities, and facilities that are easily recognizable from the air are more likely to be targeted than less notable Federal facilities.

Because an aircraft attack is by nature a suicide attack, groups which may be involved in such an attack are generally limited to extremist organizations such as al-Qa’ida. These types of groups are expected to target high profile facilities or those where mass casualties may result, such as large gathering events, hazardous materials sites (or nuclear power plants), high profile economic facilities, and national icons.

Mentally unbalanced individuals or lone wolf adversaries may also conduct such attacks on an unpredictable frequency.

Outlook

The exploitation of aircraft as weapons of mass destruction against selected targets is among the principal terrorist threats to aviation. Security enhancements since the September 11, 2001 attacks has reduced, but not eliminated, the possibility that air attacks will be attempted in the same manner. However, it is anticipated that terrorists will study and test new security procedures in an attempt to uncover weaknesses.^v

As security measures for commercial aviation continue to increase domestically and abroad, adversaries will likely turn to what they perceive to be softer targets, including GA and commercial cargo aircraft. Security measures are being increased on these industries as well, although the nature of GA makes it particularly difficult to adequately secure nationwide. The use of unmanned aerial vehicles (UAVs) or radio controlled (RC) aircraft in the future is a possibility as well. UAVs are available from more than 60 countries commercially.

7.1.3

There have been reports of Hezbollah receiving UAVs from Iran. However, the intelligence community (IC) assesses it doesn't appear to have a specific intent of conducting attacks against the United States Homeland.^{vi}

While UAVs and RC aircraft with payloads up to 25 kg are available, much smaller payloads are more common, making the UAV/RC aircraft more of a psychological weapon than one with considerable destructive power.^{vii}


- In 2004, Al-Qa'ida Islamic extremist communications mentioned the use of pilotless drones.^{viii}
- In November 2003, a container with two UAVs usually used by intelligence agencies to take spy photographs was taken into custody by Sri Lankan authorities.^{ix}

Al-Qa'ida has also reportedly considered the use of helicopters. Helicopters may be viewed as an attractive weapon due to their maneuverability and non-threatening appearance when flying at low altitudes.^x

The 2009 attempt by the Tamil Tigers to crash aircraft laden with explosives suggests that terrorists will continue to seek methods to enhance the effectiveness of an attack, particularly with smaller aircraft. Eventually, they may succeed in designing a device which will initiate on impact. In the meantime, learning from failures and successes, terrorists may enhance their attack by loading additional fuel or other combustibles into the aircraft.

References

See Section 7.32

Undesirable Event	7.2 Arson					
Definition	Accessing a facility and deliberately setting fire to the facility or to assets within the facility.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

An adversary places an improvised incendiary device containing an accelerant and utilizing a delay mechanism adjacent to a facility, but outside the view of security countermeasures.

Baseline Threat

Based on the unsophisticated nature of the attack, availability of specific information on planning and executing such an attack, the historical frequency of its use in general and specifically against Federal facilities, and demonstrated intent by terrorist organizations to utilize this tactic against Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **HIGH**.

Analytical Basis

An improvised incendiary device (IID) is a relatively inexpensive and easy device to create. IIDs are composed of commonly available ingredients such as matches, gasoline, alcohol, flammable liquids and materials or other items and designed to cause fire or intense heat as opposed to exploding. This device may be activated in the same manner as an improvised explosive device through command detonation or a timing device.

Eco-terrorists have utilized IIDs against a variety of targets, to include federal facilities and property involved in research, specifically that research involving animals, as well as land management. Through their organization's manuals, eco-terrorists have shared tactics and techniques for the construction of IIDs. Two of these manuals are entitled; *Arson-Around with Auntie ALF* and *Setting Fires with Electrical Timers: an Earth Liberation Front Guide*. Examples of such events include the following:

- In May 2009, Matthew Fraticelli and Stephanie Shinn were arrested and charged with attempted arson of a Federal facility and possession of an unregistered destructive device. The device was placed next to the facility hidden in a paper bag and placed next to the U.S. Courthouse in Sacramento, CA.^{xi}
- Al-Qa'ida operative Khalid Shaikh Mohammed admitted to a plan to destroy the Sears Tower in Chicago by burning fuel trucks in the parking garages beneath or around it.^{xii}

7.2.1

- In January 2006, three ecoterrorists were arrested in Auburn, California, in a plot to destroy federal property, cell phone towers and power generation facilities. They were arrested on January 13, 2006, in a parking lot with shopping bags containing bleach, glass cleaner, rubber gloves and masks - items that can be used to make homemade fire bombs. They were plotting to destroy U.S. Forest Service facilities, banks and commercial trucks. During the arrest, FBI agents confiscated a notebook that contained drawings of pipe bombs, lists of ingredients for creating homemade explosives and drawings of the Forest Service's Institute of Forest Genetics in Placerville.
- In 2006, Operation Backfire, a multiagency federal and state investigation led by the Federal Bureau of Investigation culminated in a 65-count indictment against eleven individuals for their domestic terrorist crimes. It covered a time period between 1996 and 2001 in the Pacific Northwest. U.S. damage related to these crimes was calculated to be tens of millions of dollars.
- The Earth Liberation Front (ELF) took responsibility for a fire on October 15, 2001, at the U.S. Bureau of Land Management's Wild Horse and Burro Facility in Litchfield, CA. A communiqué sent by ELF stated activists freed approximately 200 horses, and then set four timed incendiary devices aimed at destroying two barns, two vehicles and one office building.
- In 1998, there were two arson-related cases at the U.S. Department of Agriculture, Animal and Plant Health Inspection Service facilities in Olympia, Washington. Both of these arsons, as well as several other arson and malicious destruction cases occurred in 1998 and subsequent years on other Federal property owned by the Department of the Interior Bureau of Land Management. These crimes were committed by the (ELF) and Animal Liberation Front (ALF).
- In December 1998, at least four ELF cell members placed fire bombs at the offices of U.S. Forest Industries in Medford. When they didn't read news of any fire, they returned five days later and placed new ones, which damaged the building.^{xiii}
- In May 1997, members of an anti-government organization broke into an U.S. Internal Revenue Service office in Colorado Springs, CO. and set fire to the office. The attackers poured gasoline in filing cabinets and initiated the fire with a 15-minute timed fuse.

In 2007, 57,224 arsons were reported through the U.S. Federal Bureau of Investigation's (FBI) Uniform Crime Reporting (UCR) program. As shown in the next graph; 24,542 were of structures, and 15,984 were mobile properties.

Property Type	Offenses known
Total structure:	24,542
Single occupancy residential	10,995
Other residential	4,119
Storage	1,678
Industrial/manufacturing	269
Other commercial	2,260
Community/public	2,850
Other structure	2,371
Total mobile:	15,984
Total other:	16,698

The Department of Homeland Security's Federal Protective Service (FPS) records statistics on criminal activity in approximately 8800 General Services Administration (GSA) facilities. In both 2007 and 2008, FPS reports there were three arsons reported at GSA facilities for each year.

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI's UCR Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Target Attractiveness

Arson in Federal facilities is generally related to the nature of the work performed by the agency being targeted and may take place inside the facility itself or on the grounds. Historically, eco-terrorists pose the greatest arson threat to Federal facilities. Facilities with missions that are controversial in nature are more likely to be subject to arson, particularly missions which are contradictory to the ideology of animal and environmental organizations.

Arson is a relatively unsophisticated crime, and requires very little planning or preparation to be successful. In many cases, it is a crime of opportunity and mischief. In these cases, damage is likely to be less extensive, providing the fire is discovered in a timely manner.

The greater emphasis on planning and preparation will increase the likelihood of success, increase the amount of damage, and decrease the probability of detection. According to a Joint Special Assessment prepared by the U.S. Department of Homeland Security, FBI and the U.S. Bureau of Alcohol, Tobacco, and Firearms (ATF), and a manual published by the ELF in 2001, there are several factors which ELF/ALF takes into consideration to ensure a fire's success:

- Ensure plenty of air and fuel to feed the fire;
- Use an incendiary that supplies a prolonged and persistent heat;
- Place the incendiary device at the target's low point, to allow the fire to spread upwards;
- Use reflecting surfaces to concentrate the heat, such as corners, boxes and shelves;

- Use drafts to spread the fire rapidly (such as stairways, doorways, windows, and elevator shafts); and,
- Protect the fire from discovery through good concealment, such as the backside of a facility.

The arsonist will seek out perspective locations as part of the overall strategy to achieve success. The manual also suggests that terrorists locate cars, dumpsters, or adjacent buildings that they can readily utilize to reflect heat radiation back at a target; this tactic is particularly helpful in the event that a target building lacks any features that might otherwise help to trap or channel heat effectively.^{xiv}


Locations with remote parking lots, proximity to high crime or neglected neighborhoods, areas frequented by transients, etc., present a higher threat environment, as do remote and unattended facilities.

Outlook

The potential for eco-terrorists or other like minded extremists to utilize arson as an attack method, to include IIDs, make it likely that this type of attack will continue in the future. The frequency of attacks may increase commensurate with the frequency of Federal properties expanding into wilderness areas.

References

See Section 7.32

Undesirable Event	7.3 Assault					
Definition	Physically assaulting (with or without a weapon) a person or persons inside the facility or on the property.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Note: For the purposes of this assessment, “assault” includes crimes of violence, such as aggravated assault, homicide, forcible rape, and similar criminal acts. Incidents and synopsis of workplace violence are addressed in a separate Design-Basis Threat (DBT) summary.

Design-Basis Threat Scenario

Single assailant armed with a blunt weapon.

Baseline Threat

Based on nationwide crime statistics and the frequency of events at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **HIGH**. Crime rates vary significantly from location to location, and should be considered when characterizing this threat at a specific facility.

Analytical Basis

In 2007, 855,856 cases of aggravated assault, 90,427 forcible rapes, and 16,929 homicides (or cases of non-negligent manslaughter) were reported through the FBI’s UCR program. This represented a decrease from the number of crimes reported in 2006. Between 1988 and 2007, aggravated assaults made up approximately 61 percent of all violent crime; forcible rape approximately 6 percent; and, homicides just over 1 percent.^{xv}

An example of such an event took place on November 12, 2009, Kokou Bocco (a native of Togo), attacked three employees of the Embassy of Togo in Washington, DC with a knife before being subdued by other employees and subsequent arrest by Secret Service Officers. Bocco was inside the embassy inquiring about his return to Togo and suddenly became agitated. All three victims were taken to the hospital with non-life-threatening injuries.

Violent Crimes per 100,000 Inhabitants (2007) ^{xvi}						
Population	Aggravated Assault		Forcible Rape		Murder and Non-Negligent Manslaughter	
	Offenses known	Rate	Offenses known	Rate	Offenses known	Rate
Cities of 1,000,000 and over	105,624	418.8	6,985	27.7	2,790	11.1
Cities of 500,000 to 999,999	88,158	550.6	6,876	42.9	2,195	13.7
Cities of 250,000 to 499,999	63,994	503.2	5,716	44.9	1,455	11.4
Cities of 100,000 to 249,999	101,461	362.6	10,619	37.9	2,396	8.6
Cities of 50,000 to 99,999	81,964	277.6	9,440	32.0	1,432	4.9
Cities of 25,000 to 49,999	58,408	232.3	7,571	30.1	880	3.5
Cities of 10,000 to 24,999	52,954	208.8	7,040	27.8	746	2.9
Cities of under 10,000	50,649	243.1	5,946	28.5	532	2.6
Metropolitan Counties	145,743	231.0	14,870	23.6	2,630	4.2
Non-metropolitan Counties *	42,551	172.9	6,335	25.7	816	3.3
Suburban Areas **	239,254	211.5	26,443	23.4	3,871	3.4

* Includes state police agencies that report aggregately for the entire state.

**Suburban areas include law enforcement agencies in cities with less than 50,000 inhabitants and county law enforcement agencies that are within a Metropolitan Statistical Area. Suburban area excludes all metropolitan agencies associated with a principal city. The agencies associated with suburban areas also appear in other groups within this table.

In 2007, approximately 34 percent of all aggravated assaults reported involved use of a blunt instrument; 26 percent involved use of hands, feet, etc.; 21 percent involved use of a firearm; and, 19 percent involved use of an edged weapon. 68 percent of all murder or non-negligent manslaughter involved a firearm, perhaps attributed to the lethality of the weapon.^{xvii}

The Department of Homeland Security's Federal Protective Service (FPS) records statistics on criminal activity in approximately 8800 General Services Administration (GSA) facilities. In 2007, FPS reports there were 55 aggravated assaults and one rape in GSA facilities; in 2008 there were 35 aggravated assaults and two rapes.

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI's UCR Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Target Attractiveness

Assault is a relatively unsophisticated crime, and requires very little planning or preparation to be successful. Greater emphasis on planning and preparation may increase the likelihood of complete success or decrease the probability of detection.

Random violent criminal actions may be related to the location of the facility. Facilities in high-crime areas are more likely to face threats of assault and similar violent crime perpetrated against employees and visitors, generally as they approach or depart the facility. Locations with remote parking lots, proximity to high crime or neglected neighborhoods, areas frequented by transients, etc., present a higher threat environment.

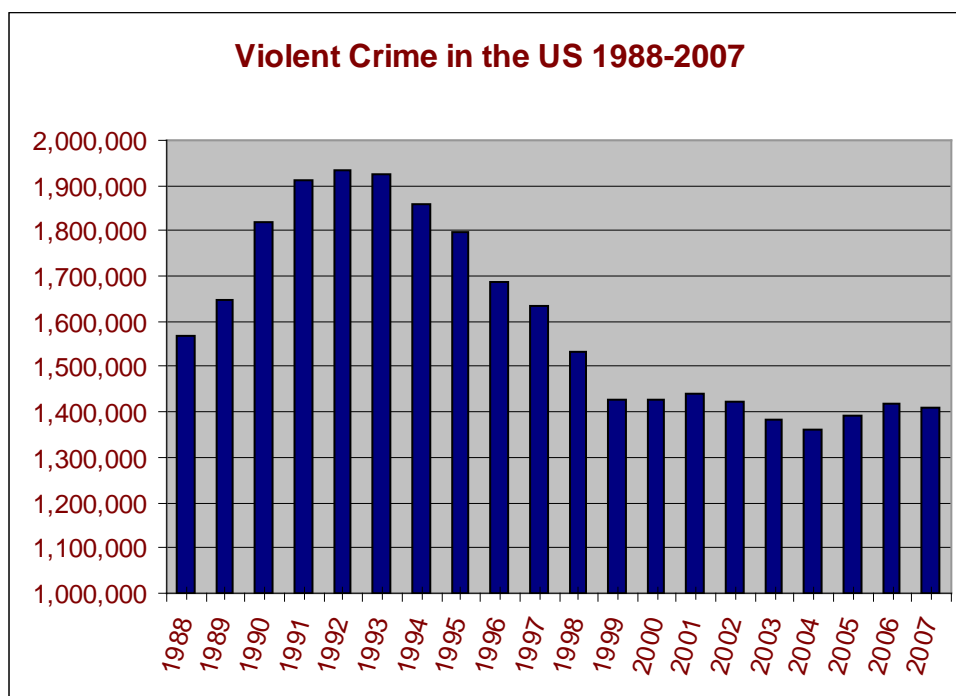
Violent crime directed at specific individuals (other than due to personal conflict outside of the work environment) is generally related to the nature of the work and may take place inside the facility itself or on the grounds. Facilities with missions that are adversarial or controversial in nature may be subject to violent criminal acts directed at specific employees or visitors, or at employees and visitors to the facility in general.

Outlook

After a peak in violent crime of about 1.9 million reported offenses in 1993, the nation has seen a reduction to approximately 1.4 million crimes, a rate that has remained fairly steady since 1999.


According to FBI statistics, violent crime overall is down 8.2 percent nationally from 1998 to 2007, with aggravated assaults down 12.4 percent and homicides down 18 percent in that 10-year period. Violent crime in all categories decreased from 2006 to 2007.^{xviii}

This trend is expected to stay relatively constant for the foreseeable future. However, local crime rates vary, even from neighborhood to neighborhood.



References

See Section 7.32

Undesirable Event	7.4 Ballistic Attack – Active Shooter					
Definition	An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

An individual enters a facility and begins to attack occupants using multiple handguns or a handgun and a rifle.

Baseline Threat

Based on the availability of firearms, the unsophisticated nature of the attack, and the historical frequency of the event specifically against Federal facilities, and well-publicized events in general, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

Active shooter scenarios are typically motivated by the desire to maximize human casualties. They are differentiated from among similar events by the indiscriminate nature of the victims targets of opportunity rather than actions directed toward a specific target. Examples include the following:

- In January 2010, at a Las Vegas Federal District Courthouse a gunman, Johnny Lee Wicks, opened fire killing one officer and wounding another. Mr. Wicks was a 66-year-old man disgruntled over cuts to his Social Security benefits. Around 8 a.m. Mr. Wicks pulled a shotgun out from underneath his black coat, and started firing indiscriminately from outside the buildings access control area. Seven federal marshals returned fire and chased the shooter from the courthouse. As he fled, Wicks was shot in the head and died. Witnesses said over 40 shots were fired over several minutes. The nine-floor courthouse hosted offices for U.S. Senators Harry Reid and John Ensign. Neither senator received any credible threats before the shooting.^{xix}
- On November 6, 2009, Jason Rodriguez entered the Legion Place office building in downtown Orlando, FL and made his way to the offices of Reynolds, Smith & Hills located on the 8th floor. Rodriguez, armed with a single handgun shot 6 employees, killing 1 and wounding 5 others. After the shooting, Rodriguez fled from the scene in his vehicle and ultimately was found a short time later at the apartment where his mother lived.

The police were able to talk him out of the apartment and into custody without incident. It was later reported Rodriguez was a former employee of the company and been fired by them in 2007. Rodriguez, who was overstressed with a myriad of problems and declining mental health, was reported to have blamed the company for “trouble with receiving his unemployment benefits” and “because they left him to rot”.

- On November 5, 2009, U.S. Army Major Nidal Malik Hasan, a military psychiatrist, armed with 2 handguns opened fire at a military processing center in Ft. Hood, TX killing 13 people and wounding 30 others before being shot multiple times by police officers. Hasan was not killed. Motives for the shooting were unclear at the time. Witnesses to the shooting stated that Hasan was shouting “Allah Akbar” before opening fire. News reports also indicated he was upset about getting ready to be deployed to Iraq, that he had been affected by the physical and mental injuries seen while treating patients and he wanted to be discharged from the Army. Hasan is also being investigated for possible ties to “terrorism”. Hasan is a U.S. citizen of Jordanian descent.
- On June 10, 2009, James von Brunn assaulted the National Holocaust Museum in Washington, DC. Von Brunn entered into the crowded building, immediately firing with a rifle, killing one guard before he was stopped by return fire.
- On April 3, 2009, a gunman in Binghamton, NY opened fire on staff and students taking an immigration test, killing 13 before committing suicide.
- On March 29, 2009, an unidentified male assailant entered a rehabilitation center in Carthage, North Carolina and attempted to find and kill his ex-wife. By the time the only police officer on duty arrived, entered the facility and stopped the gunman, eight people were dead.
- In December 2007, a gunman killed 8 people before committing suicide at a shopping mall in Omaha, NE. The gunman used an SKS assault-style rifle. He had reportedly been fired from his job, and left a suicide note.
- On April 16, 2007, a student at the Virginia Polytechnic Institute and State University School committed what has been deemed the deadliest peacetime shooting incident by a single gunman in U.S. history, on or off a school campus. In two separate attacks, Seung Hui Cho, armed with a Glock 19 and Walther P22 killed 32 people and wounded 23 others before committing suicide. Cho had previously been diagnosed with a severe anxiety disorder.
- On January 25, 1993, Mir Aimal Kasi went on a shooting spree near the entrance of Central Intelligence Agency (CIA) headquarters in Langley, Virginia. Kasi opened fire with an AK-47-style assault rifle, killing 2 CIA employees and wounding 3 others as they sat in the morning traffic. After being extradited back to the U.S. to stand trial, Kasi admitted to the shootings stating he was angry about the U.S. bombing of Iraq and CIA interference in Muslim nations.

Target Attractiveness

An active shooter is a relatively unsophisticated crime, and requires very little planning or preparation to be successful. Greater emphasis on planning and preparation may increase the likelihood of more casualties and possibly would include a wider array of weapons, to include IEDs.

Violent crime directed at specific individuals (other than due to personal conflict outside of the work environment) is generally related to the nature of the work. Facilities with missions that are adversarial in nature may be subject to violent criminal acts directed at specific employees or visitors, or at employees and visitors to the facility in general. As a determined attack, an active shooter scenario might be directed at law enforcement.

Active shooter incidents are most often perpetrated by lone wolf adversaries. A lone wolf is an individual who commits violent and/or non-violent acts in support of some group movement, or ideology, but does so alone, outside of any command structure.^{xx} The unpredictable nature of their motivations makes it difficult to determine what specific factors will make a facility or individual a more attractive target.


Outlook

Active shooter incidents are most often perpetrated by a lone wolf adversary and are thus difficult to predict or determine trends for. It is expected that random acts of violence such as the active shooter scenario will continue to be low frequency events.

The success of overseas attacks such as the coordinated and determined Mumbai attacks in 2008 suggest that in the future, the active shooter scenario may become a tactic used by determined adversaries.

References

Are in Section 7.32

Undesirable Event	7.5 Ballistic Attack – Small Arms					
Definition	Firearm fired from offsite into a facility or defined area.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

An individual armed with a rifle fires indiscriminately at a facility from outside.

Baseline Threat

Based on the unsophisticated nature of the attack, as well as the historical frequency of the event specifically against Federal facilities, and well-publicized events in general, the baseline threat to Federal facilities from this event is assessed to be **HIGH**.

Analytical Basis

Small arms gunfire may involve the use of weapons categorized as “small arms” or “light weapons”, or a combination of the two depending on the type of attack; specifically revolvers, automatic pistols, rifles, shotguns, assault rifles, light machine guns, and more. Examples of such events include the following:

- On March 4, 2010, gunman John Patrick Bedell walked up very coolly, no distress showing, and drew a weapon from his pocket and opened fire toward the teeming subway entrance to the Pentagon complex. “When he reached into his pocket, the officers assumed he was going to get a pass and he came up with a gun, Pentagon Police Chief Keevill stated. The gunman gave no clue to the officers at the checkpoint about what he was going to do. Two police officers were wounded before the assailant was shot and killed.^{xxi}
- Small arms are becoming the weapon of choice in attacks due to their availability, ease of use, transport, and concealment. In 2009 the Federal government was under the gun with weapons violations on federal properties up by 10 percent, while threats against IRS facilities climbed 11 percent.^{xxii}
- Sometime between the evening hours of October 28, 2009 and the morning hours of October 29, 2009, 4 shots were fired at the Federal Courthouse in Eugene, OR. 3 shots hit the windows of the office of U.S. Representative Peter DeFazio located on the 2nd floor, and the 4th hit the wall above the office window. Initial reporting stated uncertainty if the representative’s office was the intended target. It was speculated the shots were fired from an off ramp of a street overpass. No details were released about the type of ammunition used.

- In June 2009, a lone assailant opened fire on a U.S. Military Recruiting Office in Little Rock, AR, killing one service member and wounding another. The assailant was an American who converted to Islam.
- In May 2009, unknown gunmen on motorcycles fired on a campaign office of Iranian President Ahmadinejad (in Iran), wounding 2 adults and 1 child. No particular group was identified but terrorist were blamed.
- In July 2008, 3 gunmen identified as Turkish Nationals armed with shotguns and pistols attacked the U.S. Consulate in Istanbul, Turkey, resulting in 6 being killed (3 being the gunmen). Security camera footage showed the gunmen emerging from a vehicle used as an unlicensed taxi, killing a traffic policeman and turned running towards the consulate while firing.
- In February 2001, an accountant who had previously worked for the Internal Revenue Service and was engaged in disputes with the agency fired shots outside the White House fence. The man was firing a .38 caliber handgun.

Target Attractiveness

The use of small arms is a relatively unsophisticated attack, and requires very little planning or preparation to be successful. Greater emphasis on planning and preparation may increase the extent of damage, injuries, or deaths or decrease the probability of capture.

Random acts may be related to the location of the facility. Facilities in high-crime areas are more likely to be subject to random firearms attacks, generally from public paths of travel around the facility.


Firearms attacks directed at specific agencies are often related to controversial missions or high profile individuals, and often the tactic of hate groups or anti-governmental organizations, making tenant agency employees or visitors to the facility subject to attacks. This is a common tactic in areas such as Puerto Rico, where the attacks are directed at US government facilities by separatist adversaries. Often there is a specific event which drives the desire to carry out such an attack.

Outlook

Random small arms attacks directed at Federal facilities are expected to continue at a similar, but unpredictable frequency. Directed attacks are most often perpetrated by lone wolf adversaries. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.

References

See Section 7.32

Undesirable Event	7.6 Ballistic Attack – Standoff Weapons					
Definition	Mortar, rocket propelled grenade, etc., fired from offsite into a facility or area.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

An individual assaults a large Federal building using a homemade mortar using a fused explosive projectile.

Baseline Threat

Based on the infrequent recent history of the attack and the difficulty in effectively employing such a weapon even against a stationary target, the baseline threat to Federal facilities from this event is assessed to be **VERY LOW**.

Analytical Basis

Most countries manufacture unguided standoff weapons for their militaries, but terrorists also improvise standoff weapons with similar characteristics.

A mortar is a light artillery weapon usually with ammunition loaded through the muzzle of the barrel (or “tube”). A mortar fires a fused projectile indirectly at the target through a high-arc ballistic trajectory. The weapon fires shells at low velocities and at short range relative to other artillery weapons. The effective range of mortars and mortar systems can be from 100 meters to more than 7,000 meters.

During the Irish Republican Army’s (IRA) armed campaign against British rule in Northern Ireland, the IRA had repeatedly used homemade mortars against targets in Northern Ireland. Other examples of these types of events include:

- On November 4, 2009, in East Lansing, four Michigan State University students were arrested and charged with detonating an explosive device in the city. Police responded to a call about an explosion, where authorities said a 3-inch mortar exploded in a yard. Authorities were alerted about a car being driven by the suspects. Once stopped, a subsequent search of the vehicle yielded other explosive devices which were later destroyed by the Michigan State Police Bomb Squad.

- On February 7, 1991, homemade mortars concealed in a van with a hole cut in the roof were fired by the IRA at Number 10 Downing Street in London, England. Each shell was four-and-a-half feet long, weighed 140 pounds (60 kg) and carried a 40 pounds (20 kg) payload of the plastic explosive Semtex. No members of the cabinet were injured, but four people received minor injuries, including two police officers injured by flying debris.
- In December 1988, items used in the construction of mortars and technical details regarding the weapon's trajectory were found during a police raid of an Irish Republican Army (IRA) location in Battersea, South London.
- On November 6, 1985, a Light Anti-Armor Weapon (LAAW) rocket was fired into the 4th floor of the US Courthouse in San Juan, PR, from the 4th floor of a parking garage across the street. A Puerto Rican terrorist group claimed responsibility.
- On February 28, 1985, nine shells were launched at a Royal Ulster Constabulary facility from a Mark 10 mortar bolted onto the back of a Ford truck. Nine police officers were killed and 37 people were injured including 25 civilian police employees.
- On October 30, 1983, terrorists in San Juan, PR fired a LAAW rocket at the Federal building, striking the offices of the USDA. It is believed the FBI office in the building was the target. The LAAW was believed to have come from stocks of weapons left in Vietnam.

The intent and design of unguided shoulder-fired rockets are to counter entrenched personnel and armored vehicles at close range and to breach obstacles and penetrate fortified structures. Many countries produce such weapons. The rocket-propelled grenade (RPG) is the most common type of ammunition used and is commonly fired from a hand-held launcher based on the Russian RPG-7. The RPG-7 has many variants, and its portability and choice of warheads have made it a weapon of choice for guerrilla forces. The majority of weapons of this type are relatively light systems that a single person can carry and deploy, and they generally have a maximum effective range (powered flight) of 300 meters.^{xxiii} LAAW rockets, believed to have been obtained from old war stocks, have been used in the past as well. Weapons of this class are not very effective against structures, and are difficult to employ in urban environments due to the distance the rocket has to travel before it arms itself. Use of weapons such as this often suggests foreign involvement.

Terrorists can create improvised standoff weapons based on the materials, skills, and tools available to them. Since 2002, the Palestinian terrorist group HAMAS has used improvised Qassam rockets against Israel; these rockets are made of steel tubes filled with explosives. HAMAS terrorists reportedly hide a Qassam in a truck, drive to a clearing near the Gaza border, and launch the rocket. In addition, reporting indicates that the Irish Republican Army as of 2002 colluded with the Revolutionary Armed Forces of Colombia on the employment of improvised mortars.^{xxiv}

RPGs' are easily portable, low cost and widely available in the Middle East and Eastern Europe making them popular among terrorist groups and other sub-state militias. At this time we have not seen this type of assault on the homeland recently; but this type of attack is used extensively in many other countries, such as, Ireland, England, Iraq, and Afghanistan.

Target Attractiveness

Level IV and V facilities, national monuments and icons, highly symbolic commercial office towers, and other highly symbolic facilities are more likely to be targeted than less notable Federal facilities. Unless highly trained in the use of mortars, any attack using this type of weapon would result in random casualties and minor damage to Federal facilities.


International terrorist organizations such as Al-Qa'ida, the IRA and other terrorist organizations are expected to continue to target high profile facilities or those where mass casualties may result, such as large gathering events, hazardous materials sites (or nuclear power plants), high profile economic facilities, and national icons.

Outlook

This type of assault is primarily an overseas event at this time. It is anticipated that this may be an infrequent attack in the US in the future.

References

See Section 7.32

Undesirable Event	7.7 Breach of Access Control Point - Covert					
Definition	Use of deceit, coercion, or social engineering to gain access to a facility through a controlled entrance.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

An individual enters a Federal facility with a large group of visitors and displays a counterfeit government identification badge.

Baseline Threat

The availability of information and sources of manufacturing of false identification cards, and the historical use of fraudulent IDs as part of a criminal enterprise or for illegal purchases and identity theft, suggests significant opportunity exists to breach an access control point to commit another crime. However there is a lack of historical basis to suggest this has been commonly used with malicious intent. Consequently, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

Adversaries may use identification, whether fraudulent or legitimate, as a credential in order to obtain access to a facility for illegitimate purposes. Types of identification may include passports, driver's licenses, and social security cards.

Identification also includes more specialized forms, such as a motorcycle or pilot's license. Identification may enable adversaries to develop cover schemes, access facilities, and gain financial resources. This would allow them to operate in targeted environments without attracting unwanted attention from law enforcement agencies or security officers stationed at facility entry points. Examples of such events include:

- In February 2009, a man using a fake Matricula Consular card gained access to DHS Headquarters. He claimed he had used the card over a period of four years to access government buildings and board airliners.
- In 2003, GAO testimony revealed that over the course of several different investigations, GAO personnel were able to create and use fraudulent credentials and access federal facilities carrying firearms. Additionally, fraudulent identification was used to gain access into the U.S. through border stations and to purchase firearms.^{xxv}

7.7.1

- In September 2001, two men used stolen Belgian passports to develop a cover as journalists and gain access to Ahmed Shah Masoud, leader of anti-Taliban military forces. The men assassinated Masoud with IEDs concealed in suicide belts and camera equipment.

Target Attractiveness

Gaining access to a federal facility covertly is generally an activity related to general theft of assets, espionage, or pre-operational surveillance. Facilities which store quantities of classified or sensitive information (including proprietary private-sector data) may be targeted specifically for that information.


Facilities with higher-value assets, materials, information, etc. may face a higher threat from this type of event.

Outlook

The implementation of new measures by the Federal government, such as Homeland Security Presidential Directive (HSPD)-12, is a significant step forward in preventing the acquisition of fraudulent identification cards. Additionally, the more widespread use of electronic means of authentication of access credentials, including biometric identification, makes the creation of fraudulent credentials more challenging. However, adversary organizations continue to adapt and overcome these measures with improved technologies and techniques of their own. This is expected to present a somewhat cyclical trend in the technological effort. In general, though, the advancement in the use of technology may lead to a shift in adversary focus to the use of social engineering techniques to obtain access or steal legitimate credentials and away from attempts to create fraudulent credentials.

References

See Section 7.32

Undesirable Event	7.8 Breach of Access Control Point - Overt					
Definition	The use of force and/or weapons to defeat a personnel screening or access control checkpoint (including ID checks).					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

An adversary uses a handgun in an effort to breach security at the entrance checkpoint with the intent to proceed inside the facility.

Baseline Threat

Based on the unsophisticated nature and historic frequency of this type of event, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

The presence of a security checkpoint at the entrance to a facility does not necessarily deter adversaries from attempting to forcibly penetrate the facility. Examples of such events include the following:

- On August 21, 2009, a man was arrested attempting to breach the checkpoint at the Ron De Lugo Federal Building in the capital of Charlotte Amalie, U.S. Virgin Islands. The man was carrying a handgun.
- In June 2009, an 88 year old gunman entered the U.S. Holocaust Museum in Washington, D.C., and opened fire with a rifle killing a security officer on post at the entrance before being shot by other security officers.
- In September 2001, a Federal Protective Service Police Officer was killed by a gunman attempting to breach the checkpoint at the entrance to the Patrick V. McNamara Federal Building in Detroit, MI. The gunman was wounded by security guards.
- In July 1998, a lone gunman burst into the East entrance of the U.S. Capitol building, stormed past the magnetometer and immediately opened fire mortally wounding a police officer at the checkpoint. The gunman advanced into an interior corridor of the building and was intercepted by another police officer. The second officer was also mortally wounded before the gunman was killed by other police officers.

Target Attractiveness

Lone wolf adversaries were responsible for the majority of known attempts to forcibly breach access control points. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.


Facilities which house judges or high-profile officials, particularly those closely tied to controversial environmental or personal freedom issues may face a higher threat of this event. Also, facilities with higher-value assets, material, information, etc. may face a higher threat from this type of event.

Outlook

Improvements in technology which prevent covert attempts to obtain access using fraudulent access badges may cause determined adversaries to resort to overt attempts at breaches.

References

See Section 7.32

Undesirable Event	7.9 CBR Release – External						
Definition	Intentional release of a CBR agent into a facility through a specific access point, such as; air intake, windows, or doorways, from outside the facility.						
Original Assessment	12-17-09	Revision	0	Date	N		
Classified Annex	YES	Classification	S	Date	10-16-09		

Design-Basis Threat Scenario

A single adversary releases chlorine gas in the area of an air intake.

Baseline Threat

Based on the continuing interest and intent by certain terrorist organizations in this method of attack, mitigated by the sophisticated nature, relative infrequency, and lack of attacks against Federal facilities to date, the baseline threat to Federal facilities from this event is assessed to be **LOW**.

Analytical Basis

Al-Qa'ida leadership historically has given high priority to Chemical, Biological, and Radiological (CBR), and Chemical, Biological, Radiological, and Nuclear (CBRN) attacks to achieve mass casualty goals. In February of 2009, the Director of National Intelligence said, "Most terrorist groups that have shown some interest, intent, or capability to conduct Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRN [E]) attacks have pursued only limited, technically simple approaches that have not yet caused large numbers of casualties. Al-Qa'ida is the terrorist group that historically has sought the broadest range of CBRN [E] attack capabilities, and we assess that it would use any CBRN [E] capability it acquires in an anti-US attack, preferably against the Homeland."^{xxvi}

Domestic terrorists almost certainly lack the capability to construct and use CBRN weapons in mass casualty attacks due to the significant scientific, technical, and logistical hurdles that must be overcome. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Domestic terrorist lone offenders are more likely to use a CBRN weapon to attack within the US Homeland than domestic terrorist groups. Since January 2002, only six confirmed domestic incidents involved the attempted acquisition or production, or successful production, or actual distribution of CBRN material. All cases are known or believed to be linked to lone offenders with limited capability that operated independently and either ascribed to the ideology of a domestic terrorist movement or specifically targeted government facilities.^{xxvii}

Chlorine gas is an irritating, fast-acting and potentially deadly inhalant. It is also one of the most universal toxic chemicals, widely used in water treatment and industrial manufacturing. Chlorine is commercially available in a variety of quantities and storage methods.

7.9.1

Chlorine was effectively used in March 2007, when terrorists detonated 3 Vehicle-Borne Improvised Explosive Devices (VBIED)'s in the Anbar province of Iraq, each containing chlorine gas cylinders. The attacks killed 2 and injured over 350 people. In the two months leading up to these attacks, car bombers in Iraq had incorporated chlorine gas into 5 other VBIEDs, and a car bomb "factory" discovered by the military was found to contain numbers of chlorine cylinders.^{xxviii} Additional deadly attacks took place in April and May.^{xxix}

Al-Qa'ida and other terrorist groups have considered targeting heating, ventilation, and air conditioning (HVAC) systems of large commercial buildings.^{xxx}

While there is no evidence terrorists are planning a CBR attack from the air, Tankers or Crop Dusting type aircraft could possibly be bought or stolen to achieve this type of attack.

Domestic extremists historically have used commercially or industrially available toxic industrial chemicals, and simple dissemination techniques; their plots generally are limited in scope, aimed at a specific target, and not focused on producing mass casualties. Mass casualty attacks are almost certainly beyond their capabilities due to the scientific, technical, and logistical hurdles involved. If domestic terrorists intend to use CBRN weapons, observable indicators include procurement of lab equipment, discussions at meetings or on Web sites, recruitment of scientific or engineering experts, or performance of CBRN-related research. There is no reporting of any of these indicators.

Ricin has been the CBR weapon of choice in past domestic CBR attacks probably due to the ease of obtaining the raw materials and the ready availability of instructions on how to manufacture it in extremist literature and on the Internet. However, Ricin is unlikely to be used in an attack involving dispersal over an area because the quantity of Ricin required to achieve lethal dose over a large geographic area is significantly more than an agent such as anthrax. Anthrax is not likely to be used because production of weapons-grade anthrax is an extremely technical and hazardous process.

Individuals have attempted to acquire radiological materials—such as by harvesting material from smoke detectors—for the purpose of constructing a radiological dispersal device. This would not result in an effective radiological dispersal device because of the minimal amount of radioactive material used in smoke detectors. More highly-radioactive materials would likely be difficult to safely handle in the preparation of a package to be used in this method of attack. While there is no evidence that domestic terrorists are researching or plotting a nuclear or radiological attack, a rudimentary radiological dispersion device is within their technical capability.

Target Attractiveness

Facilities which house high-profile officials, particularly those prominent in the fight against international terrorism, or closely tied to controversial environmental or personal freedom issues may face a higher threat of this event.

An alternative to carrying hazardous materials to a site for an attack considered by adversaries is to attack facilities in close proximity to a facility. Thus, Federal facilities in close proximity to hazardous storage or transportation sites face this additional variation on this threat.

Al-Qa'ida leadership historically has given high priority to chemical, biological, radiological, and nuclear attacks to achieve mass casualty goals. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Lone wolf adversaries were responsible for the majority of known attempts to acquire, produce, or use chemical or biological materials. The targets of the plots were usually specific individuals. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.


Outlook

It is likely that international terrorist organizations such as Al-Qa'ida, along with a handful of lone offenders will continue to pursue chemical and biological materials, but most domestic terrorists will continue to have no intent or capability to use CBR weapons. Domestic terrorists who intend to use chemical or biological weapons will likely continue to prefer those that are easily produced or material which is easily obtained.

Toxic industrial chemicals and toxins probably will remain the attack method of choice for domestic actors seeking to use CBRN because of their availability and the relative ease of making them into weapons.

References

See Section 7.32

Undesirable Event	7.10 CBR Release - Internal						
Definition	Intentional release of CBR agent carried into the facility, including general interior space (lobbies) or into specific rooms or systems (HVAC rooms).						
Original Assessment	12-17-09	Revision	0	Date	N		
Classified Annex	YES	Classification	S	Date	10-16-09		

Design-Basis Threat Scenario

A single adversary releases sarin gas by dispersing it in the lobby of a Federal building.

Baseline Threat

Based on the continuing interest and intent by certain terrorist organizations in this method of attack, mitigated by the sophisticated nature, relative infrequency, and lack of attacks against Federal facilities to date, the baseline threat to Federal facilities from this event is assessed to be **LOW**.

Analytical Basis

Al-Qa'ida leadership historically has given high priority to CBR and CBRN attacks to achieve mass casualty goals. In February of 2009, the Director of National Intelligence said, "Most terrorist groups that have shown some interest, intent, or capability to conduct Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRN[E]) attacks have pursued only limited, technically simple approaches that have not yet caused large numbers of casualties. Al-Qa'ida is the terrorist group that historically has sought the broadest range of CBRN[E] attack capabilities, and we assess that it would use any CBRN[E] capability it acquires in an anti-US attack, preferably against the Homeland."^{xxxix}

Domestic terrorists almost certainly lack the capability to construct and use CBRN weapons in mass casualty attacks due to the significant scientific, technical, and logistical hurdles that must be overcome. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Domestic terrorist lone offenders are more likely to use a CBRN weapon to attack within the US Homeland than domestic terrorist groups. Since January 2002, only six confirmed domestic incidents involved the attempted acquisition or production, or successful production, or actual distribution of CBRN material. Two involved cyanide, and one involved sarin. All cases are known or believed to be linked to lone offenders with limited capability that operated independently and either ascribed to the ideology of a domestic terrorist movement or specifically targeted government facilities.^{xxxii}

Sarin has been effectively used in the past in mass-casualty attacks.

- In November 2006, Demetrius “Van” Crocker was sentenced to 30 years in prison for various violations, including the acquisition of a chemical weapon. Crocker, a self-proclaimed former member of the National Socialist Movement with a history of expressing right wing beliefs similar to those held by white nationalist extremist organizations, sought explosive materials to carry out attacks against government buildings. During the course of an FBI undercover operation, Crocker acquired an inert canister of sarin nerve gas and a block of inert C-4 explosive. Crocker told the FBI undercover agent that his “dream” was to set off a dirty bomb in Washington, DC, while Congress was in session, and he spoke of blowing up federal buildings, including a courthouse.^{xxxiii}
- On March 20, 1995, five members of Aum Shinrikyo launched a chemical attack on the Tokyo Metro. Each perpetrator carried two or three packets of sarin totaling approximately 900 millilitres of sarin. At prearranged stations, the sarin packets were dropped and punctured several times with the sharpened tip of the umbrellas. The sarin was allowed to leak out into the train car and stations and evaporate. 12 died and over 5000 were treated at hospitals.

Ricin has been the CBR weapon of choice in past domestic CBR attacks probably due to the ease of obtaining the raw materials and the ready availability of instructions on how to manufacture it in extremist literature and on the Internet. However, Ricin is unlikely to be used in an attack involving dispersal over an area because the quantity of Ricin required to achieve lethal dosage over a large geographic area is significantly more than an agent such as anthrax. Anthrax is not likely to be used because production of weapons-grade anthrax is an extremely technical and hazardous process.

Individuals have attempted to acquire radiological materials—such as by harvesting material from smoke detectors—for the purpose of constructing a radiological dispersal device. This would not result in an effective radiological dispersal device because of the minimal amount of radioactive material used in smoke detectors. More highly-radioactive materials would likely be difficult to safely handle in the preparation of a package to be used in this method of attack. While there is no evidence that domestic terrorists are researching or plotting a nuclear or radiological attack, a rudimentary radiological dispersion device is within their technical capability.

Target Attractiveness

Facilities which house high-profile officials, particularly those prominent in the fight against international terrorism, or closely tied to controversial environmental or personal freedom issues may face a higher threat of this event. In addition, facilities with large gathering areas or large volumes of visitor traffic in lobbies are more likely to be targeted.

Al-Qa’ida leadership historically has given high priority to chemical, biological, radiological, and nuclear attacks to achieve mass casualty goals. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Lone wolf adversaries were responsible for the majority of known attempts to acquire, produce, or use chemical or biological materials. The targets of the plots were usually specific individuals. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.


Outlook

It is likely that international terrorist organization such as Al-Qa'ida, along with a handful of lone offenders will continue to pursue chemical and biological materials, but most domestic terrorists will continue to have no intent or capability to use CBR weapons. Domestic terrorists who intend to use chemical or biological weapons will likely continue to prefer those that are easily produced or material which is easily obtained.

Toxic industrial chemicals and toxins probably will remain the attack method of choice for domestic actors seeking to use CBRN because of their availability and the relative ease of making them into weapons.

References

See Section 7.32

Undesirable Event	7.11 CBR Release – Mailed or Delivered					
Definition	A CBR substance or dispersal device sent to the facility through US Mail or a commercial delivery service, including an unwitting courier.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	YES	Classification	S	Date	10-16-09	

Design-Basis Threat Scenario

An envelope containing Ricin mailed to a facility.

Baseline Threat

Based on the continuing interest and intent by certain terrorist organizations in this method of attack, the unsophisticated nature and prolific literature on creating an effective agent, and the recent history of such attacks against Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

Al-Qa'ida leadership historically has given high priority to CBR, and CBRN attacks to achieve mass casualty goals. In February of 2009, the Director of National Intelligence said, “Most terrorist groups that have shown some interest, intent, or capability to conduct Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRN[E]) attacks have pursued only limited, technically simple approaches that have not yet caused large numbers of casualties. Al-Qa'ida is the terrorist group that historically has sought the broadest range of CBRN [E] attack capabilities, and we assess that it would use any CBRN [E] capability it acquires in an anti-US attack, preferably against the Homeland.”^{xxxiv}

Domestic terrorists almost certainly lack the capability to construct and use CBRN weapons in mass casualty attacks due to the significant scientific, technical, and logistical hurdles that must be overcome. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Domestic terrorist lone offenders are more likely to use a CBRN weapon to attack within the US Homeland than domestic terrorist groups. Since January 2002, only six confirmed domestic incidents involved the attempted acquisition or production, or successful production, or actual distribution of CBRN material. Half of these involved Ricin. All cases are known or believed to be linked to lone offenders with limited capability that operated independently and either ascribed to the ideology of a domestic terrorist movement or specifically targeted government facilities.^{xxxv}

There have been at least 15 incidents involving Ricin since 1997. Several targeted government personnel:

7.11.1

UNCLASSIFIED – FOR OFFICIAL USE ONLY

- On February 14, 2008, a man in Las Vegas, NV, was hospitalized in critical condition with a respiratory ailment. Two weeks later, several vials of Ricin were discovered in his hotel room.
- On February 2, 2004, Ricin was discovered on a mail-sorting machine in the Dirksin Senate office building.
- On November 6, 2003, a letter which tested positive for Ricin was discovered in the mail facility serving the White House.
- On October 15, 2003, a letter containing a vial of Ricin was discovered in the Greenville, SC, post office. The letter was addressed to the U.S. Department of Transportation (DOT), from the "Fallen Angel."
- In 2001, four letters laced with anthrax were delivered through the U.S. Mail. 5 victims died from exposure and 17 others were made ill. Hundreds more were tested or treated with prophylactic antibiotic treatments due to possible exposure. Millions of dollars were spent decontaminating government offices. Among these were the Brentwood, MD and Hamilton, NJ postal facilities. In August 2008, as the U.S. Department of Justice (DOJ) prepared to bring charges against their suspect, Dr. Bruce Ivins, Ivins took his own life.
- In November 1999, FBI agents apprehended a man in Tampa, FL, for threatening to kill court officials and "wage biological warfare" in Colorado. Upon searching his residence, agents discovered the necessary ingredients to make Ricin, though no refined Ricin was actually found. They also found test tubes and beakers, as well as the "Anarchist's Cookbook" and books on biological toxicology, in a makeshift laboratory in his home.
- On April 1, 1997, IRS investigators discovered a cache of chemicals in a residence, which included sodium cyanide, di-isopropyl fluorophosphates, and a range of corrosive acids. Computer files confiscated from the residence revealed e-mail communications that expressed a desire to obtain castor beans to extract Ricin, and the home addresses of nearly 100 federal employees from the FBI, IRS, and ATF.

Production of weapons-grade anthrax is an extremely technical and hazardous process. The use of Ricin is assessed to be more likely due to the ease of obtaining the raw materials and the availability of manufacturing instructions in extremist literature and on the internet. The manufacture of Ricin is also detailed in an Al-Qa'ida training manual.

Individuals have attempted to acquire radiological materials—such as by harvesting material from smoke detectors—for the purpose of constructing a radiological dispersal device. This would not result in an effective radiological dispersal device because of the minimal amount of radioactive material used in smoke detectors. More highly-radioactive materials would likely be difficult to safely handle in the preparation of a package to be used in this method of attack.

Target Attractiveness

Facilities which house high-profile officials, particularly those prominent in the fight against international terrorism, or closely tied to controversial environmental or personal freedom issues may face a higher threat of this event.

Al-Qa'ida leadership historically has given high priority to chemical, biological, radiological, and nuclear attacks to achieve mass casualty goals. However, since mailing quantities of a CBR agent is unlikely to result in mass casualties, this is an unlikely tactic for use by international terrorist organizations.

Domestic terrorist groups show little interest in a sophisticated CBR capability. While there is no evidence that domestic terrorists are researching or plotting a nuclear or radiological attack, a rudimentary radiological dispersion device is within their technical capability.

Lone wolf adversaries were responsible for the majority of known attempts to acquire, produce, or use chemical or biological materials. The targets of the plots were usually specific individuals. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.

Mail-handling facilities and employees, while not necessarily the target of a mailed CBR substance, may be unintentional victims due to incidental exposure to the substance during normal handling and processing of the mail. As such, the threat to such a facility is considerably higher.


Outlook

Ricin will probably remain the CBR weapon of choice for a mailed package, unless new technologies make it easier to manufacture and distribute others. Domestic terrorists who intend to use chemical or biological weapons will likely continue to prefer those that are easily produced or material which is easily obtained.

It is likely that international terrorist organization such as Al-Qa'ida, along with a handful of lone offenders will continue to pursue chemical and biological materials, but most domestic terrorist groups will continue to have no intent or capability to use CBR weapons.

References

See Section 7.32

Undesirable Event	7.12 CBR Release – Water Supply					
Definition	Intentional release of a CBR agent into a building's potable water supply, from a location outside the building.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	YES	Classification	S	Date	10-16-09	

Design-Basis Threat Scenario

One to three adversaries access on-site potable water supply piping at a valve without backflow protection and pump a highly lethal, tasteless, odorless agent into the system under pressure.

- OR -

At a facility with large water storage tanks or a reservoir, adversaries access the water supply and dump a non-lethal contaminant into the water.

Baseline Threat

Based on the continuing interest and intent by certain terrorist organizations in this method of attack, the unsophisticated nature of the event, suspected and disrupted plots, ease of access, and availability of contaminants (both lethal and non-lethal, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

Al-Qa'ida leadership historically has given high priority to CBR and CBRN attacks to achieve mass casualty goals. In February of 2009, the Director of National Intelligence said, "Most terrorist groups that have shown some interest, intent, or capability to conduct Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive (CBRN [E]) attacks have pursued only limited, technically simple approaches that have not yet caused large numbers of casualties. Al-Qa'ida is the terrorist group that historically has sought the broadest range of CBRN [E] attack capabilities, and we assess that it would use any CBRN [E] capability it acquires in an anti-US attack, preferably against the Homeland."^{xxxvi}

Domestic terrorists almost certainly lack the capability to construct and use CBRN weapons in mass casualty attacks due to the significant scientific, technical, and logistical hurdles that must be overcome. Domestic terrorist groups show little interest in a sophisticated CBR capability.

Domestic terrorist lone offenders are more likely to use a CBRN weapon to attack within the US Homeland than domestic terrorist groups. Since January 2002, only six confirmed domestic incidents involved the attempted acquisition or production, or successful production, or actual distribution of CBRN material. All cases are known or believed to be linked to lone offenders with limited capability that operated independently and either ascribed to the ideology of a domestic terrorist movement or specifically targeted government facilities.^{xxxvii}

7.12.1

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Most biological agents are susceptible to routine water treatment, and most chemical agents require a substantial quantity to be effective. A 1999 study identified 5 CB agents which could be potentially added to a water supply that are tasteless, odorless, have a strong resistance to chlorine, are soluble and stable in water, are sufficiently lethal to cause casualties in small doses, and are readily available worldwide, making them effective in an attack against potable water supplies.^{xxxviii} Although unclassified, the list of agents is provided in the Classified Annex to this report.

Municipal water systems are designed to protect against naturally occurring bacterial, parasitic, and viral agents, not determined terrorist attacks. However, some biological agents would survive even substantial chlorination. In order to be most effective, contamination would need to take place after the water treatment steps and as close as possible to the target in order to limit the amount of dilution.

Adversaries have demonstrated an interest in and the capability to access water supply facilities and contaminate potable water supplies. These include the following events:

- In mid-August 2006, a walk-in source to the FBI reported two individuals in El Paso County, Colorado discussed contaminating a private water system owned by an identified corporation that serves approximately 240 homes and an elementary school. One of the individuals was upset over alleged harassment by the corporation and the El Paso County Sheriff's office. The other individual is a member of a known "sovereign citizens" group. The individuals knew how to contaminate the system and were aware of such details as the fact that it operated at low pressure and that they might need a pump to succeed.^{xxxix}
- In September 2005, intrusions were reported at several water towers in Washington and Idaho. Locks were cut, protective vents were removed, ladders were climbed, and fences were breached in the intrusions.^{xl}
- In May 2003, a fatwa posted on an Islamic website justified the poisoning of U.S. water supplies.^{xli}
- In March 2003, several surveillance cameras at a Kentucky water facility were turned away from their views of a storage tank and facility entrances. Upon investigation, it was determined that an adversary had scaled a fence and accessed the top of a storage tank.^{xlii}
- In 2002, papers seized during the arrest of a Lebanese national in Seattle included "instructions on poisoning water sources" from a London-based Al-Qa'ida recruiter.
- In 1978, water supplies in Phoenix, AZ were intentionally contaminated with typhoid.^{xliii}
- In 1977, water supplies in Miami, FL were contaminated with what was purported to be botulism toxin.^{xliv}
- In 1972, members of the right-wing organization Order of the Rising Sun attempted to attack water supplies in St. Louis, MO and Chicago, IL with approximately 30-40 kilograms of typhoid bacteria.^{xlv}

In 2006, the U.S. Environmental Protection Agency (EPA) concluded that unintentional backflow contamination events go largely undetected, are not investigated, are not properly documented, or are not reported. In 2002, the EPA conducted a study to trace and assist in verifying the ease with which someone could inject contaminants into a drinking water distribution system. This tracer study demonstrated that contaminants could easily be introduced into a system through either direct connection or backflow from a service connection.

Contamination of water supplies may also be intended as a denial of service attack, or as a demonstrative but relatively harmless event. Any contamination of water supplies will lead to significant public reaction, so the terrorists' motivation does not necessarily have to be to kill or injure occupants at a specific facility. Contaminating water in a reservoir would have such an effect, even though the water would still be treated before entering the public's potable water supply.

Target Attractiveness

Water reservoirs and facilities with large water storage tanks likely face a higher threat of a denial of service or simple contamination event. Facilities which house high-profile officials, particularly those prominent in the fight against international terrorism, or closely tied to controversial environmental or personal freedom issues may face a higher threat of a directed attack.

Lone wolf adversaries were responsible for the majority of known attempts to acquire, produce, or use chemical or biological materials. The targets of the plots were usually specific individuals. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.


Outlook

It is likely that international terrorist organizations such as Al-Qa'ida, along with a handful of lone offenders will continue to pursue chemical and biological materials, but most domestic terrorists will continue to have no intent or capability to use CBR weapons. Domestic terrorists who intend to use chemical or biological weapons will likely continue to prefer those that are easily produced or material which is easily obtained.

Toxic industrial chemicals and toxins probably will remain the attack method of choice for domestic actors seeking to use CBRN because of their availability and the relative ease of making them into weapons.

References

See Section 7.32

Undesirable Event	7.13 Civil Disturbance					
Definition	Deliberate and planned acts of violence and destruction stemming from organized demonstrations on or near Federal property.					
Original Assessment	12-17-09	Revision	0	Date		
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

During a planned demonstration, a subset of protesters turn violent and use available on-site materials to attempt to breach or damage the entrance to the facility.

Baseline Threat

The frequency of organized protests at Federal facilities is high; however, historically very few organized protests have turned particularly violent. Consequently, the baseline threat to Federal facilities from this type of event is assessed to be **MODERATE**.

Analytical Basis

Civil disturbance is one of the primary tactics of nonviolent resistance. Given its place at the boundary of fidelity to law, it is said to fall between legal protest, on the one hand, and conscientious refusal, revolutionary action, militant protest, and organized forcible resistance on the other hand. Examples of these events include:

- September 2008, In Kansas City anti-war marchers broke the glass and attempted to set a police car on fire. They also broke the windows out of buildings in the area.^{xlvi}
- December 2007, In New Orleans, LA, police had to resort to less-than-lethal weapons to disperse a crowd during protests against a City Council plan to tear down low-income New Orleans housing.^{xlvi}
- In November 1999, black-clad anarchists from Eugene, Oregon planned and conducted deliberate vandalism of corporate properties in downtown Seattle in conjunction with the World Trade Organization meetings.

Some protesters practice the non-violent form of civil disorder with the expectation that they will be arrested. Some expect to be attacked or even beaten by the authorities. Protesters often undergo training in advance on how to react to arrest or to attack, so that they will do so in a manner that quietly or limply resists without threatening the authorities.

Major protests against Federal facilities are usually planned in advance and known to local law enforcement resources.

7.13.1

In most cases where demonstrations at overseas embassies and consulates have turned violent, attempts to cause damage to, or force entry into their facilities have generally involved only materials found on site. Only in rare cases did the demonstrators bring specific tools for use in attempting damage or breaching.

Target Attractiveness

Facilities which are highly symbolic of or directly involved in controversial environmental, personal freedom, or international relations issues face a higher threat to this event, and may be subject to larger and more frequent demonstrations. Specific Federal facilities are often the scenes of protests related to causes of which the facility is representative. For example, State Department facilities are often targeted for protests against U.S. involvement in overseas interests or even military actions, and courthouses become the scene of protests related to court decisions.


In areas where the number and variety of Federal facilities is limited, the largest and most obvious Federal facility may become a frequent site of protests against any governmental action, regardless of the cause.

Outlook

Organized demonstrations at Federal facilities are expected to continue on a routine basis, and some are likely to turn into violent civil disturbances with unpredictable regularity.

References

See Section 7.32

Undesirable Event	7.14 Coordinated or Sequential Attacks					
Definition	A planned assault on a facility that integrates the aspects of several undesirable events.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Note: A “coordinated” attack is one which involves several adversaries acting in concert. A “sequential” attack is one where adversaries attack in “waves” to overcome layered defenses.

Design-Basis Threat Scenario

Assault by a team of 4-12 adversaries, each armed with an assault-style rifle and handgun. The assault may be of a suicidal nature and will also involve the use of small IEDs.

Baseline Threat

Based on the current lack of demonstrated or expressed intent on behalf of adversarial organizations to carry out such an attack in the US, and the limited number of adversary organizations willing to undertake suicide missions in the US, the baseline threat to Federal facilities from this type of event is assessed to be **LOW**.

Analytical Basis

Coordinated attacks are strikes designed to increase ferocity and chaos. The ability to conduct a coordinated attack shows high levels of operational and technical sophistication. In a conventional sense, a coordinated attack could be the moving of multiple units and/or devices into the same target area or a large simultaneous campaign involving many units and/or devices. Insurgents and terrorists utilize coordinated attacks in different ways. Some experts consider coordinated attacks to be the hallmark of Al-Qa’ida, although it is and can be utilized by any group with superior planning and operational experience.^{xlviii} Examples of these events include:

- In July 2009, 8 to 15 suicide attackers mounted assaults on government compounds in two towns in Afghanistan, killing six and wounding four members of the Afghan security forces. In one of the towns, coordinated attacks on 3 government compounds involved the bombers attacking in waves in an attempt to penetrate the security barriers.^{xlix}
- Also in July 2009, the Mexican Drug cartel “La Familia” launched a series of coordinated commando attacks/ambushes against federal police and Mexican soldiers in Mexico. The ambushes occurred in eight cities and involved convoys of gunmen springing surprise attacks on government positions. The cartel gunmen were noted as being a disciplined force backed with military-grade assault rifles and grenades.¹

- A CD-ROM seized in 2008 by Belgian authorities and provided to Interpol is a detailed audio explanation by now-deceased senior Al-Qa'ida operative Yousef al-Ayeeri of a method taught in an Al-Qa'ida training camp for attacking a publicly accessible building. Al-Ayeeri recommended assembling a team of 12 individuals, each armed with an assault rifle and grenade and carrying approximately 20 kilograms of explosives. The attackers are to storm the building, seal off escape and access points, and occupy it long enough to set and detonate their explosive packages. Al-Ayeeri stressed the importance of carrying out these steps before law enforcement can respond, even if notified early in the attack. He assumed the attackers will be killed during the operation. Al-Ayeeri believed attackers would be able to enter many publicly accessible buildings easily with little or no resistance from often poorly trained and lightly armed or unarmed security guards.^{li}Interpol believes the Arabic-language recording was made shortly before al-Ayeeri's death in 2003.
- In November 2008, terrorists conducted a series of coordinated attacks encompassing 10 locations throughout Mumbai, India, killing at least 195 people and wounding more than 325. Two hotels and another building were seized with hostages taken. The terrorists displayed thorough operational planning encompassing command and communication while carrying out these attacks.

Sequential attacks have been used to first penetrate perimeter defenses and then follow-up with assaults on personnel or assets inside a protected facility.

- In September, 2008: Terrorists attacked the U.S. Embassy in Sanna, Yemen, with two VBIEDs followed up with gunmen on foot who attempted to exploit a breach in the perimeter wall.
- In September, 2006: Four terrorists detonated a VBIED outside the U.S. Embassy in Damascus, Syria, and attempted to storm the compound.

Target Attractiveness

In order to assure the greatest possibility of success, it is assessed that high profile targets that appear to be well-defended are unlikely to be targeted for such an attack. However, the target facility would likely have to be of some prominence or importance in order to create the psychological impact sought by adversaries carrying out a complex coordinated attack.


High profile facilities with significant protective measures in place, or facilities with high-value assets protected by security-in-depth measures, may be subject to sequential attacks, with “waves” of adversaries used to overcome layered defenses.

Outlook

No such attack has ever been carried out in the U.S. However, the success of international terrorist organizations in such attacks overseas suggests that the U.S. may experience this type of attack in the future.

References

See Section 7.32

Undesirable Event	7.15 Disruption of Building & Security Systems					
Definition	Physically accessing building or security systems for the purpose of disrupting or manipulation of the systems.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	Yes	Classification	S	Date	10-16-09	

Note: This assessment does not include cyber attacks. Prevention of cyber attacks are outside the scope of this document.

Design-Basis Threat Scenario

One to three adversaries gain access to the power supply to several of a building's CCTV cameras with the intent to disable the cameras.

Baseline Threat

Based on the unsophisticated nature of this event, mitigated by the infrequent use against Federal facilities, the baseline threat to Federal facilities from this type of event is assessed to be **LOW**.

Analytical Basis

The disruption of building and security systems has not been an activity terrorists focus on. It is possible that lone wolf adversaries may want to conceal their identity by disabling a facility's building or security system, when committing a crime of theft or burglary.

An example of such an event took place in March 2003, when several surveillance cameras at a Kentucky water facility were turned away from their views of a storage tank and facility entrances. Upon investigation, it was determined that an adversary had scaled a fence and accessed the top of a storage tank.^{lii}

Terrorists prefer to engage in major structural sabotage in order to cripple services, transportation systems, or other types of critical infrastructure, rather than just disrupt a building's operating systems. Structures may also be targeted irrespective of whether direct casualties will be inflicted. For instance, the primary consideration of an attack on a major power grid may not be inflicting casualties directly from the attack; rather, the aim is to cripple the structure itself in order to paralyze critical services.

Target Attractiveness

The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility an attractive target. However, Federal facilities, national monuments and icons, and highly symbolic commercial office buildings are all more likely to be targets for lone wolf or terrorists to attempt to disable a building or security system in order to carry out another type of undesirable event.

7.15.1


Terrorist sources also discuss the vulnerabilities of specific structures and the optimal locations for device emplacement in order to disrupt building systems and infrastructure. The U.S. bombing prevention community can preempt these attacks by understanding the structural weaknesses of the critical infrastructure and work on hardening efforts to protect them. Local authorities should catalog points of critical infrastructure such as utility and energy facilities, bridges, dams, and national monuments and icons and ensure that all possible safeguards are in place given available resources.

Outlook

Trends show that attacks or plots on structures and facility systems are usually aimed at bridges, tunnels, oil refineries, and maritime ports indicating that the attackers conducted diligent surveillance for extended periods of time. The suspect in the Brooklyn Bridge Plot surveyed the bridge to determine the best location to sever cables with a blowtorch. Multiple terrorist resources stress the importance of continued surveillance before an attack on critical infrastructure.^{liii}

References

See Section 7.32

Undesirable Event	7.16 Explosive Device – Mailed or Delivered					
Definition	An explosive device sent to the facility through US Mail or a commercial delivery service, including an unknowing courier.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

A package approximately the size of a shoebox containing a pipe bomb is initiated by opening the package.

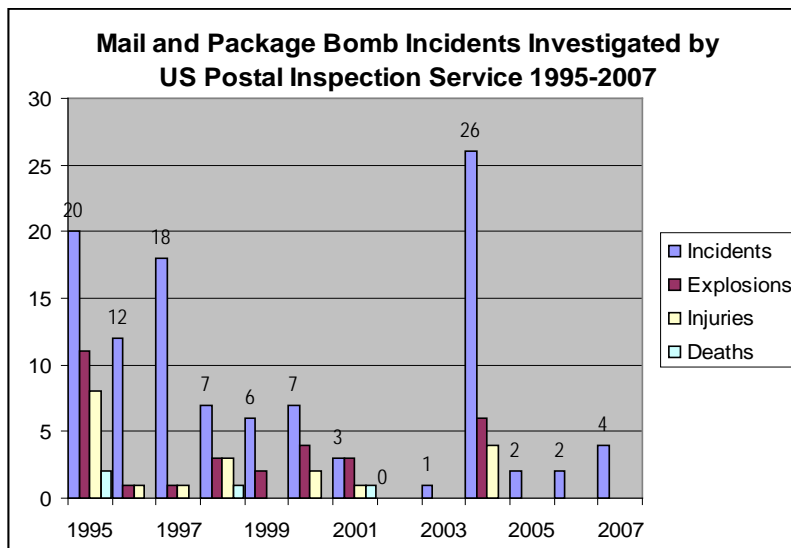
The pipe bomb will be PVC-type pipe to reduce weight, and contain approximately two pounds of black or smokeless powder. The device will also contain added shrapnel, such as nails or metal ball bearings (BBs). Black or smokeless powder has an approximate TNT equivalency factor of 0.55. 2 pounds of black powder would have a TNT equivalency of 1.1 pound of TNT.

Baseline Threat

Based on the unsophisticated nature of the attack, availability of components and instructions, and the history of its use in attacks against Federal officials, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

The U.S. Postal Inspection Service investigated at least 108 incidents of mail or package bombs between 1995 and 2007.



7.16.1

Examples of these events include the following:

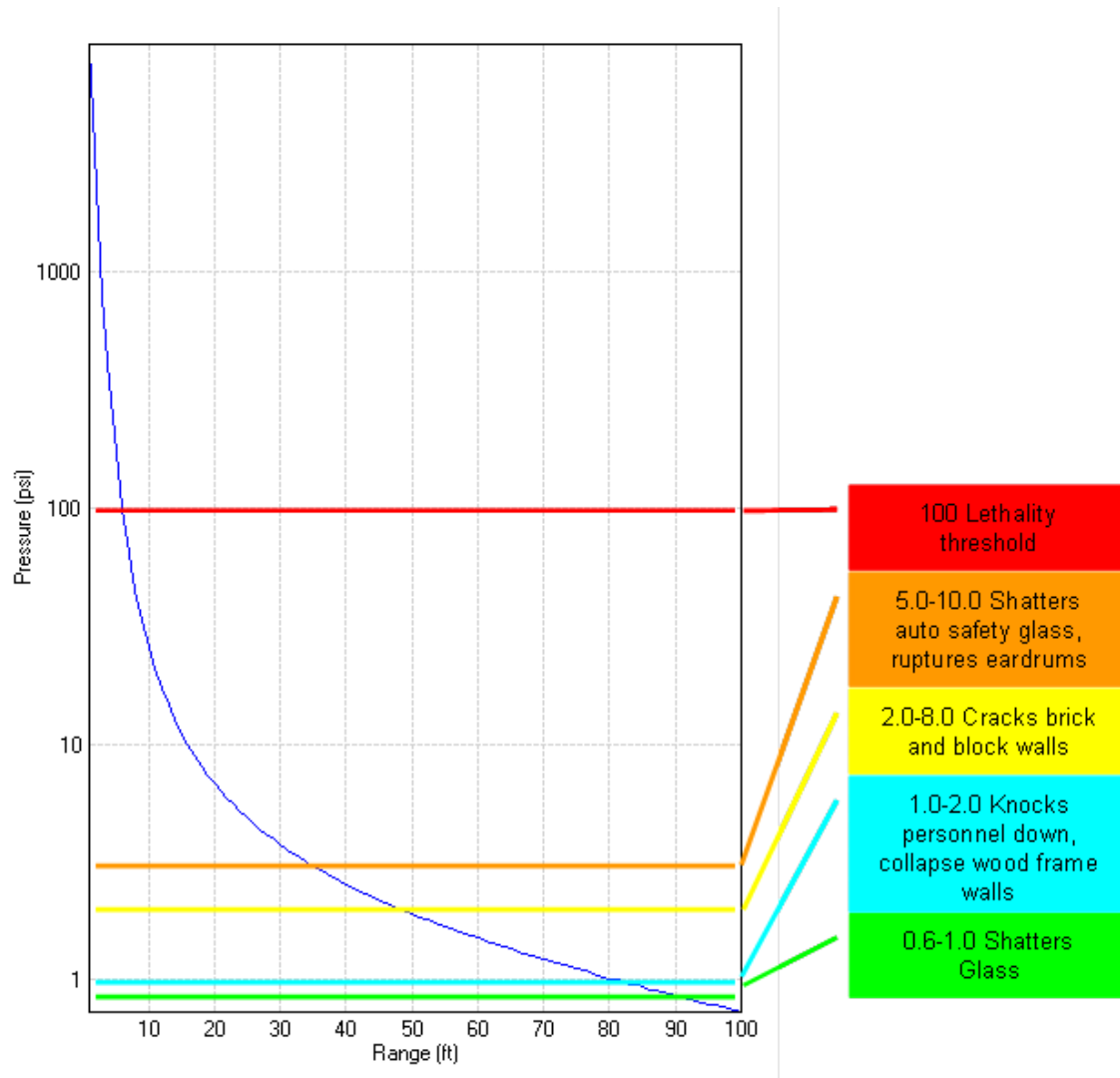
- In January and February 2007, a bomber called “The Bishop” sent several unassembled bombs to financial firms in the United States. The devices in the packages were pipe bombs, with the firing circuits not fully connected. Each package contained a letter stating, “[t]he only reason you are still alive is because I did not attach one wire.”
- From 1975-1998, Theodore “Ted” Kaczynski sent 16 bombs to targets including universities and airlines, killing three people and injuring 23. The devices made use of smokeless powder, black powder, and ammonium nitrate.
- On September 4, 1991, an Albany, New York resident R. VanGorden Stedman was injured when he opened a mail bomb. A 24-year-old unemployed Ulster County New York man was later arrested.
- In 1991, a postal worker processing mail in Dumfries, Virginia noticed a suspicious mail package in a collection box. The package was later determined to be a mail bomb sent by a former spouse of the intended addressee.
- In December 1989, Walter Leroy Moody, Jr. sent four package bombs through the mail. The first killed Judge Robert S. Vance of the United States Court of Appeals for the 11th Circuit and seriously injured his wife at their home near Birmingham, Alabama. Two days later, civil rights attorney Robert Robinson was killed by a similar device. A third device, sent to the federal courthouse in Atlanta, was intercepted and defused by ATF bomb technicians. A fourth was defused after being mailed to the Jacksonville office of the NAACP. Moody’s motive was a long-festering resentment of the court system from a conviction and failed appeals. His contact with Judge Vance in a 1980s case led to even deeper resentment and a personal animus that led to revenge. The FBI determined that the other bombs were meant to make them suspect that racism was the motive. Each bomb included a steel pipe filled with Red Dot double-base smokeless powder, finishing nails secured to the outside of the pipe, and a detonator fashioned from a flashbulb filament with distinctive wiring and a ballpoint pen casing. The detonators from the two bombs that did not explode contained a green small arms powder identified as high explosive primer. Three of the bombs also had welded end plates that were joined together by a steel rod through the center of the pipe. Moody had been convicted in a 1972 case involving a pipe bomb with a design similar to that of the 1989 bombs.

A 2001 study by the FBI suggests a number of conclusions may be drawn about improvised explosive devices used in the U.S.:

- Gunpowder and black powder are among the most commonly used as the explosive charge. These propellants are easily purchased on the commercial market.
- The most commonly used container is galvanized pipe, followed by PVC pipe.

- When shrapnel is added to the device, the type varies based on adversary ingenuity and available materials. BBs and other small pieces of hardware are common, as is glass or even gravel.

Overpressure Curve for 2 Pounds of Black or Smokeless Powder



Target Attractiveness

Lone wolf adversaries were responsible for the majority of known attempts to deliver a letter or package bomb. The targets of the plots were usually specific individuals. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.

A study of bomb-related offenders by the FBI identified nine primary motives of adversaries. The two motives most applicable to sending a letter or package bomb are ideology (against a specific activity or function of a particular facility) and revenge against society of individuals. Facilities which house judges or high-profile officials, closely tied to controversial social, environmental, political, or economic issues may face a higher threat of this event.

Mail-handling facilities and employees, while not necessarily the target of a package bomb, may be unintentional victims due to premature detonation since they are intended to intercept such a device. As such, the threat to the facility is considerably higher.

According to ATF statistics from 2004 to 2007, California consistently has the highest number of bombing incidents, three to four times higher than states with the next most frequent number.

Outlook

The number of actual incidents over the past 25 years is low, and expected to continue at that rate.

It is projected that the letter and package bombs may trend toward smaller packaging as the necessary components continue to be miniaturized. For example, greeting cards now provide a power source and a switch in one small package. The limiting factor continues to be smaller initiators (smaller than a standard blasting cap) and the availability of explosives which are powerful in smaller amounts, such as military-grade sheet explosives.

The use of more powerful homemade explosives is also likely in the near future. The use of peroxide-based explosives such as Hexamethylene Triperoxide Diamine (HMTD) and Triacetone Triperoxide (TATP) are anticipated, increasing the power of the explosives and facilitating the decrease in size of devices.

References

<https://www.tripwire-dhs.net/>


<http://www.securitymagazine.com/>

<http://www.albany.edu/sourcebook/pdf/t400012007>

USDOJ/OIG Special Report, the FBI Laboratory: An Investigation into Laboratory Practices and Alleged Misconduct in Explosives-Related and Other Cases (April 1997)

Behavior and Characteristics of Bomb Related Offenders, National Center for the Analysis of Violent Crime, FBI Academy, June 2001.

Overpressure curve calculated using A.T.-Blast version 2.2

Undesirable Event	7.17 Explosive Device – Man-Portable External					
Definition	An explosive device placed on the property, outside of a building and left to detonate after the adversary departs.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

A device concealed in a backpack near an entrance to the facility.

The IED will consist of approximately 4 pounds of black or smokeless powder in galvanized pipe bombs. The device will also contain added shrapnel, such as nails or metal ball bearings (BBs). The device may also contain steel plates used to direct the force of the explosive towards the entrance. The device will be detonated by a timer mechanism. Black or smokeless powder has an approximate TNT equivalency factor of 0.55. 4 pounds of black powder would have a TNT equivalency of 2.2 pounds of TNT.

Baseline Threat

Based on the unsophisticated nature of the attack, availability of materials and instructions, presence of multiple adversary groups who are known to use it as a tactic, disruption of recent plots, and historical frequency of events, including those directed at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

IED attacks are the favored method of most terrorist groups around the world. Man-portable improvised explosive devices (MPIEDs) are generally used to target people rather than structures. Examples of these events include the following:

- In September 2009, the FBI disrupted a plot to bomb the Paul Findley Federal Building and Courthouse in Springfield, IL. A U.S. citizen with proclaimed ties to Al-Qa'ida was arrested. During the planning for the attack, the adversary considered carrying a backpack IED into the facility or planting one outside.^{liv}
- On May 5, 2008, a pipe bomb exploded outside of the Edward J. Schwartz Federal Courthouse in San Diego, CA. The explosion caused damage to the front entrance and lobby, as well as buildings across the street. The device consisted of three pipe bombs, two measuring two inches in diameter and ten inches in length, and one measuring 1-1/2 inches in diameter and 10 inches in length. The explosive used was Pyrodex®, a black powder propellant. The device also contained approximately 110 ½-inch roofing nails for added fragmentation. The IED was contained in a back pack, which was soaked in gasoline. The adversary threw a match on the backpack, causing it to ignite, and subsequently causing the device to initiate.

7.17.1

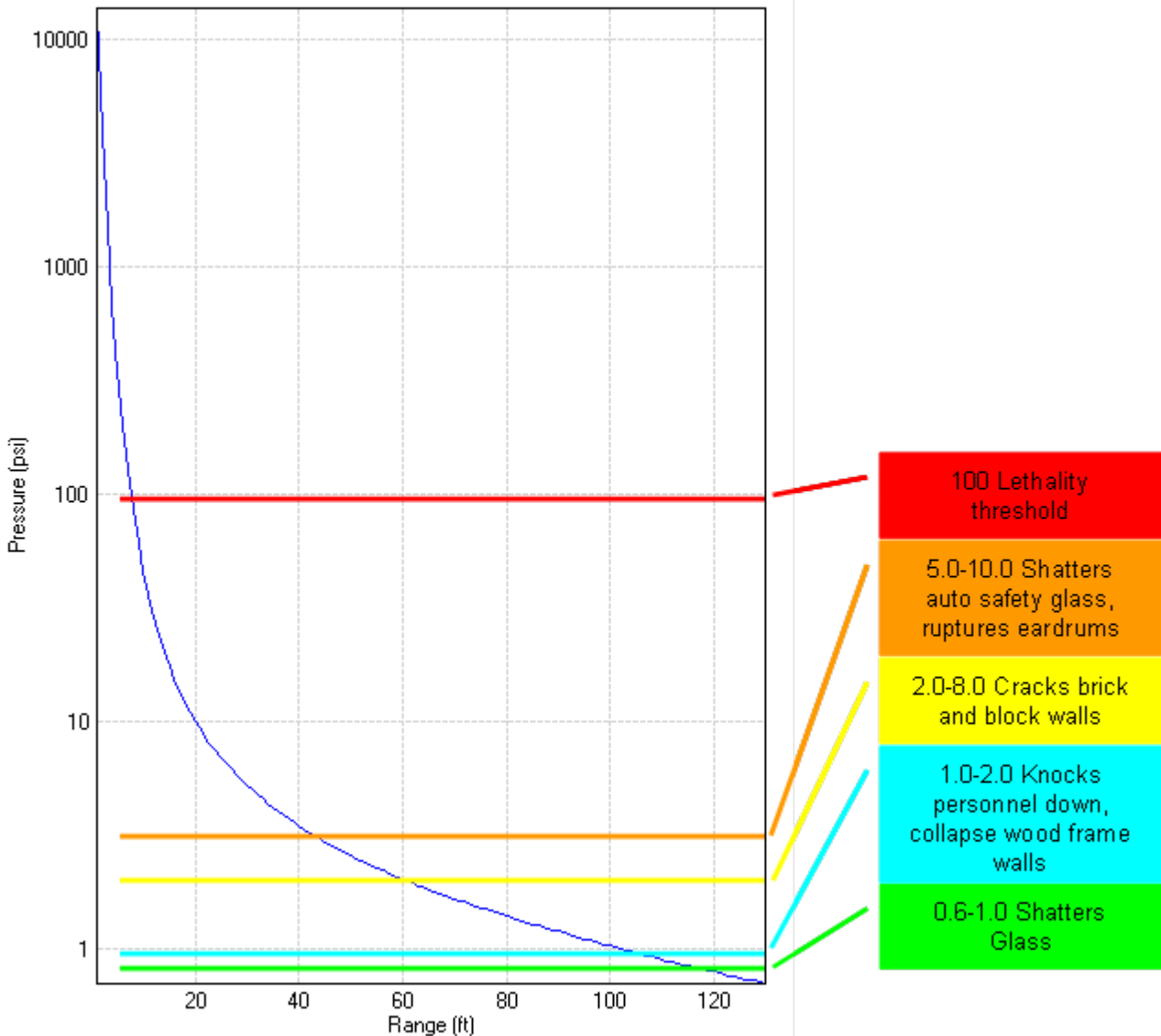
UNCLASSIFIED – FOR OFFICIAL USE ONLY

- On March 5, 2008, an IED contained in an ammunition box exploded in front of the armed forces recruiting station in New York City's Time Square. The case is still under investigation.
- On July 27, 1996, two people were killed and 111 injured in the Centennial Olympic Park in Atlanta, Georgia during the 1996 Summer Olympics. Eric Robert Rudolph planted a green U.S. military field pack containing three pipe bombs made up of 3-4 pounds of smokeless powder surrounded by nails. The device was initiated by an alarm clock. Steel plates were included to direct the force of the blast. Rudolph used similar devices in bombings of an abortion clinic in the Atlanta suburb of Sandy Springs on January 16, 1997; the Otherside Lounge in Atlanta on February 21, 1997, and an abortion clinic in Birmingham, Alabama on January 29, 1998. Rudolph's other devices utilized dynamite for the explosive charge.

A 2001 study by the FBI suggests a number of conclusions may be drawn about improvised explosive devices used in the U.S.:^{lv}

- Gunpowder and black powder are among the most commonly-used explosives. These propellants are easily purchased on the commercial market.
- The most commonly used container is galvanized pipe, followed by PVC pipe.
- When shrapnel is added to the device, the type varies based on adversary ingenuity and available materials. BBs and other small pieces of hardware are common, as is glass or even gravel.

Overpressure Curve for 4 Pounds of Black or Smokeless Powder



Target Attractiveness

Lone wolf adversaries were responsible for a large number of known IEDs used in the U.S. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.

A study of bomb-related offenders by the FBI identified nine primary motives of adversaries. The two motives most applicable to sending a letter or package bomb are ideology, (against a specific activity or function of a particular facility), and revenge against society of individuals. Facilities which house high-profile officials, closely tied to controversial social, environmental, political, or economic issues may face a higher threat of this event.

High-profile and highly-symbolic facilities and facilities which have large public gathering spaces may face a higher threat of this event.

According to ATF statistics from 2004 to 2007, California consistently has the highest number of bombing incidents, three to four times higher than states with the next most frequent incidents.


Outlook

The use of man-portable IEDs by both international terrorists' overseas and domestic terrorists within the U.S. continues to be a frequent occurrence, although targeting of federal facilities is infrequent. However, we assess that the use of a man-portable IED placed outside of a Federal facility to continue to be a likely type of terrorist attack.

The use of more powerful homemade explosives is also likely in the future. The use of peroxide-based explosives such as HMTD and TATP are anticipated, increasing the power of the explosives without a commensurate increase in size.

References

See Section 7.32

Undesirable Event	7.18 Explosive Device – Man-Portable Internal					
Definition	An explosive device carried into the building by an adversary or an unsuspecting occupant, visitor, or courier, and left to detonate after the adversary departs.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

A device concealed in a backpack is placed in a public area inside a facility.

The IED will consist of approximately 4 pounds of black or smokeless powder in galvanized pipe bombs. The device will also contain added shrapnel, such as nails or metal ball bearings (BBs). The device may also contain steel plates used to direct the force of the explosive towards the entrance. The device will be detonated by a timer mechanism. Black or smokeless powder has an approximate TNT equivalency factor of 0.55. 4 pounds of black powder would have a TNT equivalency of 2.2 pounds of TNT.

Baseline Threat

Based on the unsophisticated nature of the event, availability of materials and instructions, presence of multiple adversary groups who are known to use it as a tactic, disruption of recent plots, and historical frequency of events, including those directed at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

IED attacks are the favored method of most terrorist groups around the world. MPIEDs are generally used to target people rather than structures. Examples of these events include the following:

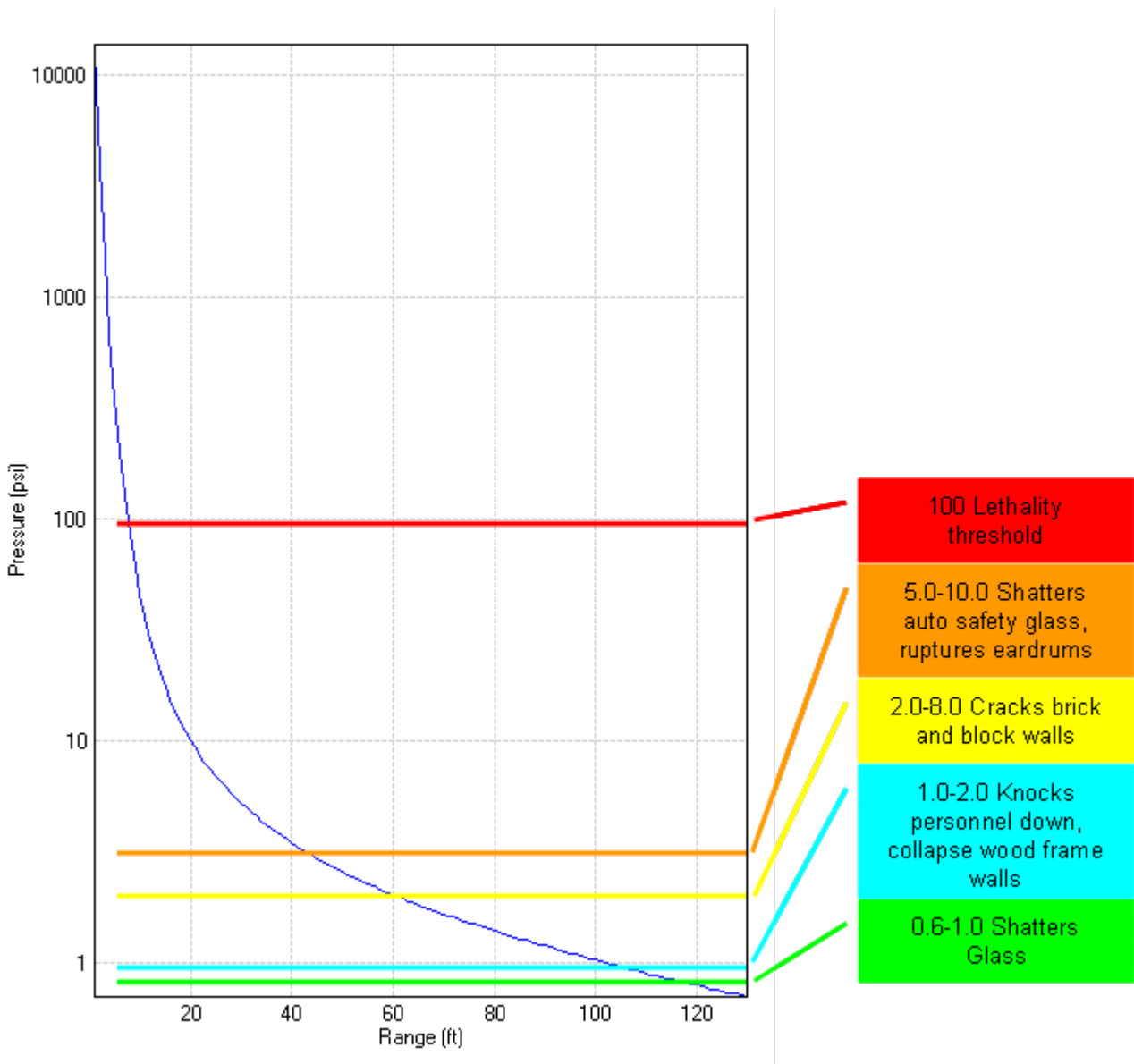
- In September 2009, the FBI disrupted a plot to bomb the Fountain Place Tower in Dallas, TX. The Fountain Place Tower is a high rise commercial facility housing a number of bank offices, as well as more than 200,000 square feet of space leased by the General Services Administration on behalf of the Environmental Protection Agency. A Jordanian citizen was arrested. During the planning for the attack, the adversary considered planting a backpack IED in a public restroom in the facility, and located a suitable site during reconnaissance. The adversary stated he wanted to attack the foundation of the building from within the facility.^{lvi}
- In September 2009, the FBI disrupted a plot to bomb the Paul Findley Federal Building and Courthouse in Springfield, IL. A U.S. citizen with proclaimed ties to Al-Qa'ida was arrested. During the planning for the attack, the adversary considered carrying a backpack IED into the facility and conducted surveillance inside the building. In recorded conversations with an undercover agent, the adversary said he felt it would be difficult to smuggle a backpack device past building security.^{lvii}

- In April and May 2009, the U.S. Government Accountability Office (GAO), conducted a test by smuggling fake bomb parts, liquid explosives and low-yield detonators, into several high-profile federal facilities across the country.^{lviii}
- On June 20, 2005, a man carrying a hand grenade and shouting threats was shot dead by police in the lobby of the federal courthouse in Seattle, WA. A man described as angry about child support rulings against him, entered the lobby of the courthouse and was observed by a guard removing the grenade from his backpack. After 25 minutes of negotiating with police, the man made what was perceived to be a threatening movement at which time officers had no choice but to fire. It was discovered the grenade was “inert”, but there was no way the police could tell as the man held it.^{lix}
- On March 9, 2000, federal agents arrested Mark Wayne McCool after he bought 1.4 lbs. of C-4 plastic explosives and an automatic weapon from an undercover FBI agent. He planned to attack a Houston federal building which he believed housed offices of the FBI and the Bureau of Alcohol, Tobacco and Firearms.^{lx}
- In 1999, Kenneth Carter, Bradford Metcalf, and Randy Graham, who were members of the North American Militia of Southwestern Michigan, were convicted on charges relating to conspiring to use firearms and explosives to destroy federal buildings in Battle Creek, Mich., kill federal agents, and assassinate politicians.^{lxi}

A 2001 study by the FBI suggests a number of conclusions may be drawn about improvised explosive devices used in the U.S.:

- Gunpowder and black powder are among the most commonly-used explosives. These propellants are easily purchased on the commercial market.
- The most commonly-used container is galvanized pipe, followed by PVC pipe.
- When shrapnel is added to the device, the type varies based on adversary ingenuity and available materials. BBs and other small pieces of hardware are common, as is glass or even gravel.

Pressure Graph for 4 Pounds of Black or Smokeless Powder



Target Attractiveness

Lone wolf adversaries were responsible for a large number of known IEDs in the U.S. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.

A study of bomb-related offenders by the FBI identified nine primary motives of adversaries. The two motives most applicable to sending a letter or package bomb are ideology, (against a specific activity or function of a particular facility), and revenge against society or individuals. Facilities which house high-profile officials, closely tied to controversial social, environmental, political, or economic issues may face a higher threat of this event.

Facilities with high volumes of visitor traffic are more likely to be targeted using this tactic due to the ability of an adversary to blend in on entry.

As with most terrorist attacks, high-profile and symbolic facilities likely face a higher threat to this event.

According to ATF statistics from 2004 to 2007, California consistently had the highest number of bombing incidents, three to four times higher than states with the next most frequent incidents.


Outlook

The use of man-portable IEDs by both international terrorists' overseas and domestic terrorists within the U.S. continues to be a frequent occurrence, although targeting of Federal facilities is relatively infrequent. However, we assess that the use of a man-portable IED placed outside of a Federal facility to continue to be a likely type of terrorist attack.

The use of more powerful homemade explosives is also likely in the future. The use of peroxide-based explosives such as HMTD and TATP are anticipated, increasing the power of the explosives without a commensurate increase in size.

References

See Section 7.32

Undesirable Event	7.19 Explosive Device – Suicide/Homicide Bomber					
Definition	An explosive device carried into the facility by an adversary with the intent of reaching a specific target or area then detonating, killing or injuring the bomber and others.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	YES	Classification	S	Date	10-16-09	

Design-Basis Threat Scenario

A suicide/homicide bomber enters an occupied public space in the facility and detonates a suicide vest. The device consists of five pounds TNT equivalent of explosive, activated by a switch carried by the adversary. The type of explosive is known to vary widely. The device will also contain added shrapnel, such as nails, screws, nuts and bolts, or metal ball bearings (BBs).

Baseline Threat

Based on the unsophisticated nature of the attack, availability of materials and instructions, disrupted plots, and a history of suicide terrorism events occurring outside the continental United States; intelligence sources suggests some willingness by terrorists, however because this type of event has not happened in continental United States, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Analytical Basis

The prevalence of suicide bombings in the United Kingdom, Afghanistan, Pakistan, Iraq, Jordan, Saudi Arabia, and other countries demonstrate that suicide bombing is a preferred terrorist method of attack. These types of attacks appear to be a calculated choice by operational planners. Terrorists probably are drawn to suicide bombings because they are effective, efficient, inexpensive, and easier to execute than other tactics. Since the bomber usually dies during the mission, suicide attacks also reduce the danger of captured operatives revealing important information under interrogation.^{lxii} Examples of these events include the following:

- In August 2006, UK authorities disrupted a terrorist plot to smuggle liquid components of an explosive on board several aircraft, assemble full devices in flight, and detonate them en route from the United Kingdom to the United States.
- On July 7, 2005, suicide bombers detonated three bombs within one minute of each other on different London subway cars. A fourth terrorist's device detonated on a London bus. All four terrorists were killed, as were 52 other persons, and 700 persons were wounded. The devices were made of peroxide-based explosives.^{lxiii}

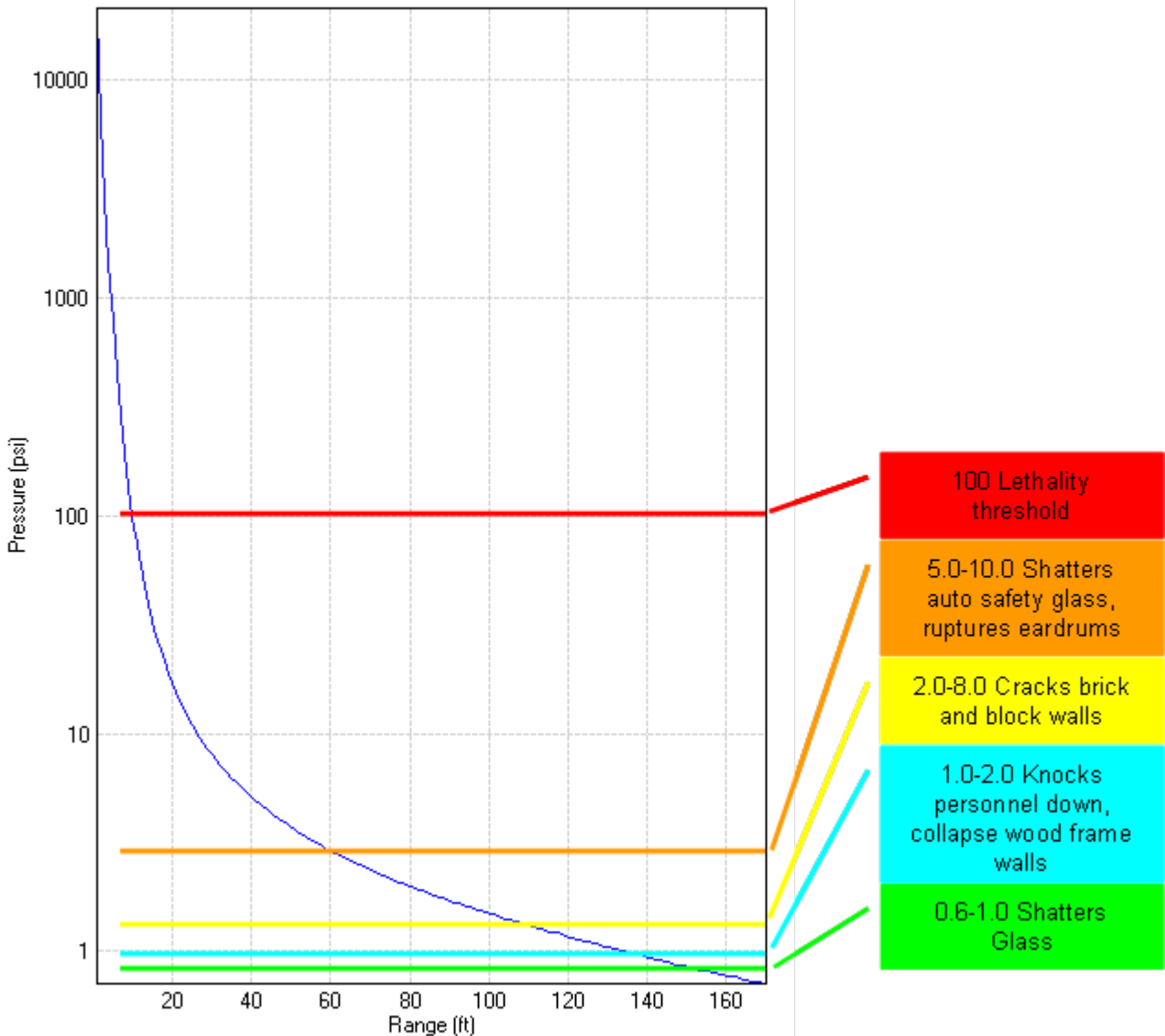
- In 1997, a Palestinian immigrant named Ghazi Ibrahim Abu Maizar came within hours of detonating a suicide vest in a Brooklyn, N.Y. subway station. Police found two fully rigged pipe bombs packed with nails and bullets in his apartment.

While suicide bombings have not taken place in the U.S., suicide terrorism has manifested itself in the U.S. in other forms:

- On January 5, 2002, 15-year-old Charles J. Bishop deliberately flew a Cessna 172 into the Bank of America tower in Tampa, FL. A note found in the plane stated “Osama bin Laden is absolutely justified in the terror he has caused on 9-11. He has brought a mighty nation to its knees! God blesses him and the others who helped make September 11th happen.”
- In 2002, Al-Qa’ida planned a suicide hijacking to attack the U.S. Bank Tower/Library Tower in Los Angeles. Jemaah Islamiya (JI), al-Qa’ida’s Southeast Asian terrorist affiliate, was to provide Southeast Asian men as operatives to avoid arousing suspicion; the terrorists were planning to use shoe bombs to gain access to the cockpit.
- On September 11, 2001, al-Qa’ida terrorists seized control of 4 commercial passenger airliners with the intent of deliberately crashing them into iconic targets in the United States. Three aircraft reached their targets: the World Trade Center towers in New York City and the Pentagon outside of Washington, DC. The fourth crashed into a field in Shanksville, PA after passengers attempted to retake control of the aircraft.

The size and makeup of suicide vests vary. A variety of explosive types are used, from military- and commercial-grade explosives to more powerful improvised explosives in differing quantities. Unless the attack is being targeted against a specific individual and the bomber has the opportunity to get close enough for the blast effect alone to kill, the primary effect of the vest design is to spread shrapnel.

Overpressure Curve for 5 Pounds of TNT Equivalent Explosive



Target Attractiveness

Suicide bombers suggest a high level of dedication to a cause in which death is a reward or seen as an acceptable end to a means. Thus it is a tactic currently reserved to the most dedicated extremist organizations and high-profile and highly-symbolic facilities, and facilities which have large public gathering spaces or high volumes of visitor traffic may face a higher threat of this event.

Based on the guidance provided in a terrorist planning document recovered in 2005, a suicide bomber planning an attack in the United States may choose a target that is easily accessible, allowing the individual to enter quickly and self-detonate before security and potential victims can react.^{lxiv}

7.19.3

Lone wolf extremist and even mentally unstable individuals cannot be discounted. The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary.

Outlook


Some experts disagree, but largely due to the prevalence and success of such attacks overseas, it is anticipated that this tactic will be used against targets in the U.S. in the future, possibly by lone wolf adversaries or unstable individuals as opposed to organized extremist groups.

Suicide bombers are resorting to more creative means of concealing their devices. Female suicide bombers have used suicide belts or vests and also have strapped large amounts of explosives to their stomachs, allowing them to operate under the guise of pregnancy. In August 2009, a suicide bomber attempted to assassinate the Assistant Interior Minister of Saudi Arabia with a device concealed inside a body cavity and activated by cell phone.

The use of more powerful homemade explosives is also likely in the future. The use of peroxide-based explosives such as HMTD and TATP are anticipated, increasing the power of the explosives without a commensurate increase in size.

References

See Section 7.32

Undesirable Event	7.20 Explosive Device – Vehicle Borne IED					
Definition	An attack against a facility that utilizes a vehicle to deliver an improvised explosive device.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

In a location where vehicles are not subject to screening for VBIEDs, a passenger sedan with an ammonium-nitrate based charge of 200 pounds of TNT equivalency concealed in the trunk, initiated by a timer or other delay mechanism such as a fuse.

In a location where vehicles entering are subject to screening for VBIEDs by use of physical inspection of the trunk, passenger compartment, undercarriage, etc., a passenger sedan with an ammonium-nitrate based charge of 50 pounds of TNT equivalency concealed in sealed void spaces (door panels, gas tank, etc.), initiated by a timer or other delay mechanism.

The ammonium-nitrate mix is known to vary, which may result in substantially different TNT equivalency factors.

Baseline Threat

Based on the unsophisticated nature of the attack, availability of materials and instructions, presence of multiple adversary groups who are known to use it as a tactic, disruption of recent plots, and historical frequency of events, including directed at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**.

Based on the lack of historical examples in the U.S., probable suicidal nature of the attack, as well as terrorist planning documents which suggest parked devices are a preferred tactic, the baseline threat to Federal facilities of a VBIED ramming attack is assessed to be **VERY LOW**.

Analytical Basis

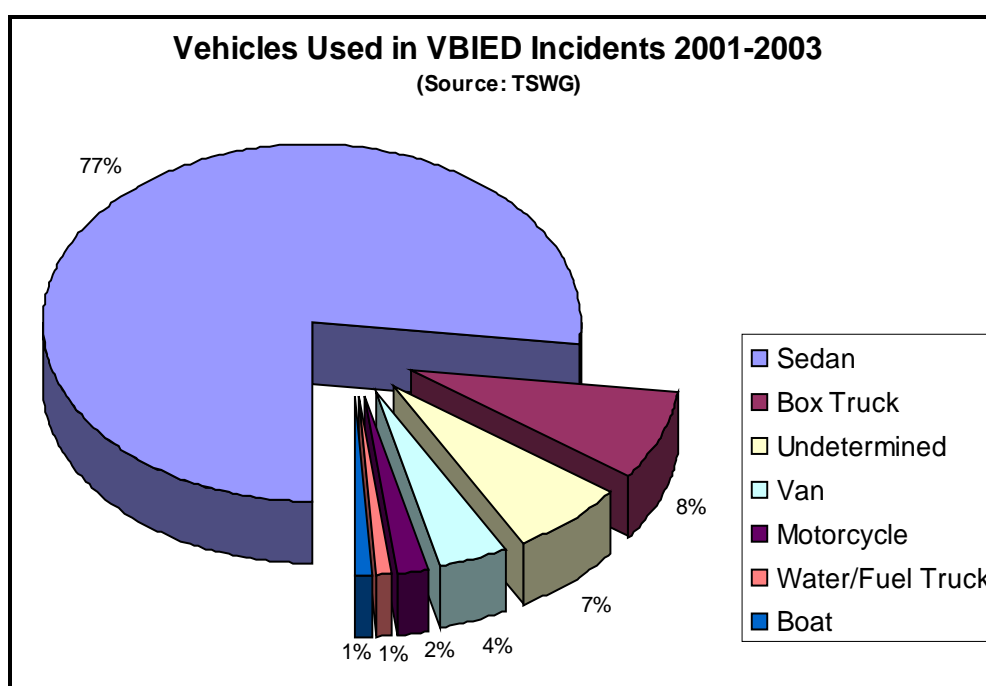
The VBIED is used by virtually all terrorist organizations. It is an attractive attack option for terrorists as it provides a large, mobile device capable of causing significant damage and/or casualties. It is the most likely terrorist device to cause mass casualties.

Approximately 77 percent of VBIEDs in a three-year period involved sedan type vehicles, with the type depending upon local availability, the ability to blend into the surroundings, ease of conversion, and terrorist preference; 8 percent involved box trucks, and 4 percent involved passenger or cargo vans. (See the TSWG graph on next page)

Sedans are easily obtainable and may be purchased new or used from dealers or through private sales. Purchasing passenger vehicles does not normally alert law enforcement or intelligence agencies of a potential problem. Passenger vehicles may also be stolen; according to the FBI's Uniform Crime Reports, automobiles made up approximately 73 percent of all stolen vehicles in 2007. Additionally, passenger vehicles tend to cause less suspicion than other commercial type vehicles and could be parked next to Federal facilities or in some cases within underground parking garages beneath Federal facilities without question.

Vehicle ramming as a method of positioning a vehicle-borne improvised explosive device has yet to be attempted in the U.S. Adversaries will generally try and place the VBIED as close to the facility as possible in order to maximize its effect. In order to achieve this, the adversary may use an innocuous vehicle that does not raise any suspicions. Adversaries may also park the VBIED at night or at times when security around the target is reduced.

Finally, the anticipated explosive payload is well within the carrying capacity of sedans.



In a study conducted by the U.S. State Department and the Technical Security Working Group (TSWG), 70 percent of explosive loads for VBIEDs were between 20 and 200 pounds (TNT equivalent), 20 percent were between 200-2000 pounds, and the remaining 10 percent were over 2000 pounds.

80 percent of VBIED explosive loads are concealed in the trunk, 15 percent are located within the passenger compartment, and 5 percent are concealed in other void spaces or are in an open vehicle cargo area.

All types of explosive have been used in VBIEDs. Conventional military or commercial explosives are sometimes used in small VBIEDs (up to approximately 50 pounds) or as booster charges for improvised explosive loads. In some cases, including the bombings of two U.S. Embassies in East Africa in 1998, commercial grade explosives have been used to form the main charge.

Improvised explosives, especially ammonium nitrate-based explosive mixes, are the preferred option for terrorists for the main explosive load in VBIEDs. This is because improvised explosives are relatively easy to manufacture in large quantities and can be manufactured from easily obtainable materials. The following improvised explosives are commonly encountered:

- Ammonium Nitrate and Fuel Oil (ANFO) is extensively used as the main charge in VBIEDs across the world and is favored by Al-Qa'ida. The constituent parts are easy to obtain and the explosive is relatively simple to manufacture.
- Ammonium Nitrate and Aluminum (ANAL) is also widely used for car bombs with the aluminum providing added effect. ANAL was used extensively by PIRA in VBIEDs during the 1970s and 1980s and more recently by Al-Qa'ida.
- Ammonium Nitrate and Nitrobenzene (ANNIE) has also been used in VBIEDs across the world. ANNIE has been used by PIRA and by Far Eastern terrorist groups in the past.
- Ammonium Nitrate and Sugar (ANS) is not yet widely used but has become the explosive of choice for VBIEDs and other large IEDs deployed by PIRA and dissident republican terrorists. Car bombs in London and Birmingham, England in 2001 contained ANS.
- TriAcetone TriPeroxide (TATP) has been favored by Hamas in their attacks on Israeli targets, was used by Richard Reid (the "shoebomber"), and has been used in VBIED attacks in London and elsewhere. TATP can be easily prepared in a basement lab using commercially available starting materials. However, it is extremely sensitive and can result in accidental detonation.
- SE Asian groups and Jemaah Islamiyah in particular seem to have concentrated their efforts on Potassium Chlorate based explosives, possibly mixed with TNT, and also mixed, according to some reports, with sulphur and aluminum.

Although the use of manufactured explosive material is more reliable, the use of ordinary household items may be used to construct IEDs making it easier for the perpetrator to evade detection. The Internet has been and is currently being used to facilitate recruitment of others who share a radical ideology, to provide propaganda, and to share ideas, knowledge and training. Tactics discussed on the Internet by terrorists include how to construct and use VBIEDs.

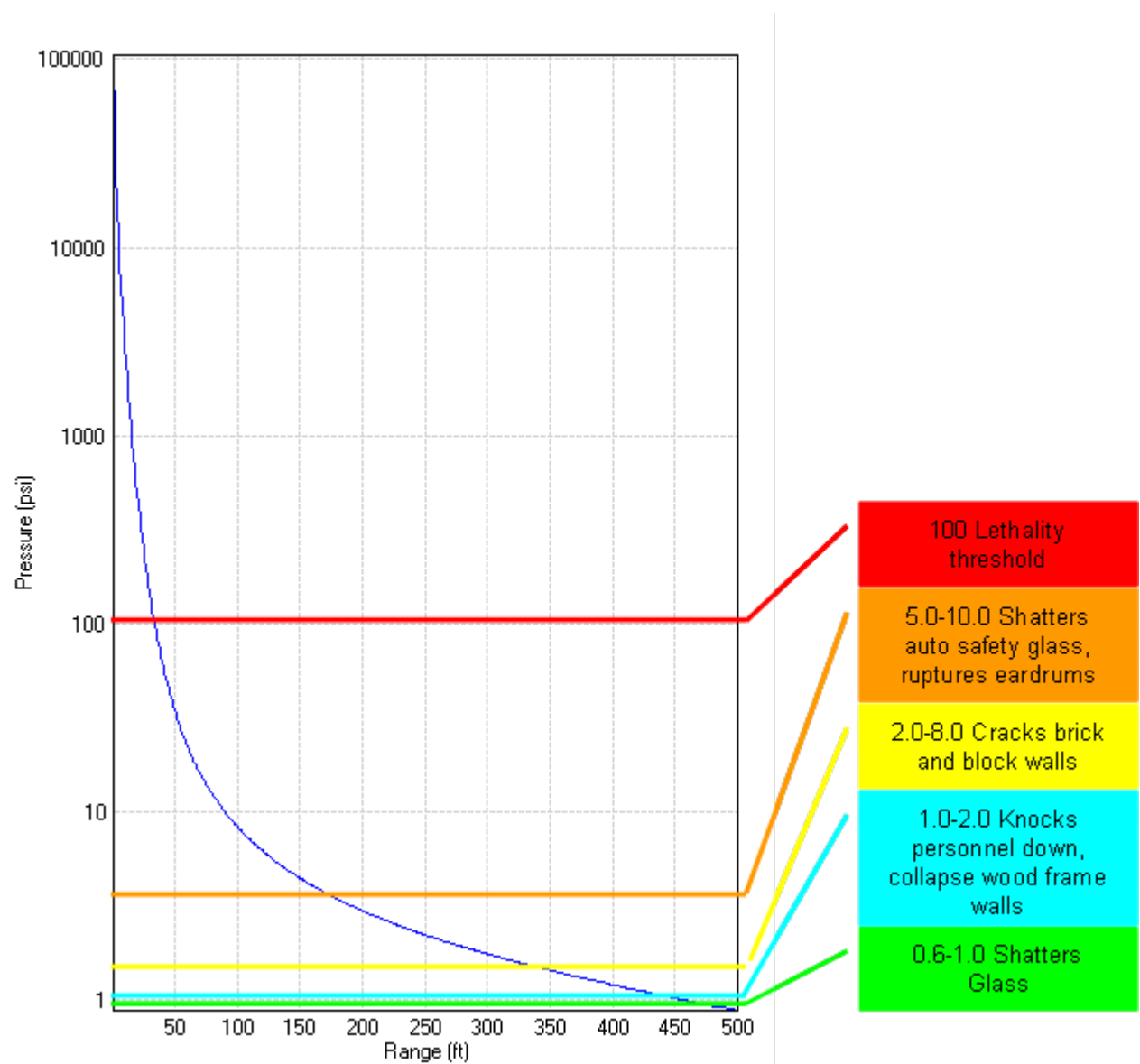
Initiation of VBIEDs may be by timing mechanism, command initiation using cell phones or pagers, or victim-operated (booby trap) activation. Nearly 50 percent of all VBIEDs over a three year period were timer initiated. In its simplest form, a timed VBIED is initiated with a burning fuse. This method was used by Ramzi Yousef to initiate the bomb inside the World Trade Center in 1993, and by Timothy McVeigh to initiate the bomb outside the Murrah Federal Building in Oklahoma City in 1995.

International and domestic terrorists as well as lone-wolf adversaries and others desiring to use violence as a means to an end have demonstrated the continued capability and intent of using motor vehicles laden with explosives to attack U.S. government facilities and other targets both stateside and abroad. Examples of these events include the following:

- On September 24, 2009, the FBI made an arrest of a U.S. citizen which disrupted a plot to utilize a car bomb against the Paul Findley U.S. Federal Building and Courthouse in Springfield, IL. A non-functional device provided by the FBI was in a van which the adversary parked at the curb of the target. The device was set to “function” with a cell-phone initiator. The same day, the FBI arrested a Jordanian citizen (a registered alien); ending an unrelated plot to attack a commercial bank building in Dallas, TX which housed a sizeable Environmental Protection Agency in leased space (the intended target was the banking center, with desired impacts on the financial sector). The FBI provided an inert VBIED consisting of ANFO with Composition-4 (C-4 military grade explosive) boosters in a Sport Utility Vehicle (SUV), which the adversary then drove and parked in the underground garage. Both adversaries had declared ties to Al-Qa’ida. In both cases, the adversary’s initial plan was to use a man-portable device brought inside the facility. Their plans subsequently changed to more effective vehicle bombs.
- On September 17, 2008, two passenger vehicles designed as IEDs attacked the U.S. Embassy in Sana’a, Yemen. One vehicle was painted to match local police vehicles and its passengers wore Yemini Security Forces uniforms. As this vehicle passed the embassy, the occupants opened fire with automatic weapons. A second vehicle then attempted to penetrate the embassy security gate but was impeded by the security gate and security personnel. This vehicle then detonated near the embassy perimeter wall. One of the attackers, was wearing a suicide explosive vest, and was killed prior to being able to detonate the device. Several Yemeni security forces along with civilians outside of the embassy were killed.
- On August 7, 1998, two truck bombs detonated, almost simultaneously, outside the United States Embassies in Tanzania and Kenya. These attacks killed over 230 people, including 12 Americans, and injured over 4000. The two bombs consisted of over 2000 pounds of explosives each. Trinitrotoluene or TNT was the main explosive used in both bombs. In Kenya, the TNT was inserted into several hundred small cylinders and mixed with aluminum nitrate and aluminum powder wired to detonating cord which was connected to batteries and a detonating switch located in the truck cab. The explosives were packed into some twenty specially designed wooden crates that were sealed and then placed in the bed of the trucks. In Tanzania, the TNT was attached to multiple oxygen tanks and gas canisters and then surrounded by bags of ammonium nitrate fertilizer. Sand was also used to serve as a crude or improvised shape charge in an attempt to direct the blast.

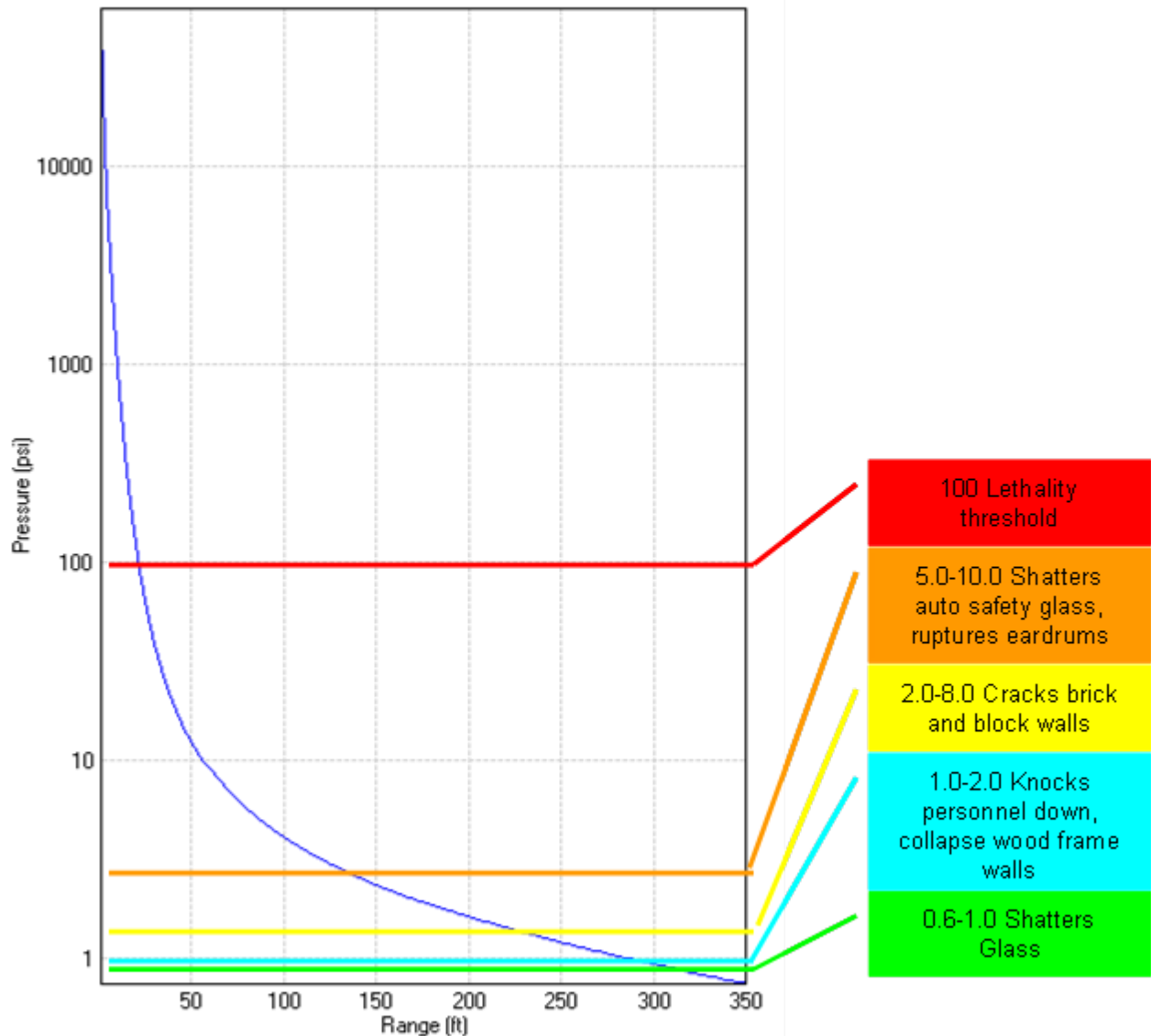
- On August 2, 1998, an unidentified subject drove a pickup truck containing an explosive fuel mixed bomb into the Tippecanoe County Courthouse in Lafayette, Indiana. The subject then lit the fuse and fled. A possible subject who held anti-government views was identified. The device was constructed of 3 large barrels of gasoline and other ignitable liquid. A propane tank was filled with smokeless powder, wood shavings and other chemicals and components. Approximately 15 feet of detonating cord, safety fuse and a flare was used as the initiator.
- On April 19, 1995 a rental truck laden with explosive materials was detonated outside the Oklahoma City Federal Office Building resulting in 168 fatalities including children. The blast reportedly destroyed or damaged 324 buildings within a 16-block radius and destroyed or burned 86 vehicles. The Ryder truck used held 13 barrels that had been fastened to floorboards nailed to the truck. Each barrel when filled with the explosive mixture weighed approx. 500 pounds. Materials used were 108 bags of explosive-grade ammonium nitrate fertilizer, three (3) 55-US gallon drums of liquid nitromethane, several crates of explosive Tovex, 17 bags of ANFO, and spools of shock tube and cannon fuse. McVeigh had arranged the barrels in the truck to form a shaped charge.
- On February 23, 1993 a rental van laden with explosives was driven into the underground parking garage for the World Trade Center complex and detonated. The explosion caused six fatalities, over a thousand injuries and significant damage to the World Trade Center complex to include Tower 6, the U.S. Customs House (GSA leased building) and several other GSA leased sites. The explosives used in the attack consisted of urea nitrate as the main charge combined with other metals, to include aluminum and magnesium as well as boosters consisting of nitroglycerine, ammonium nitrate dynamite and smokeless powders.

Overpressure Curve for 200 Pounds of TNT Equivalent Explosive



7.20.6

Overpressure Curve for 50 Pounds of TNT Equivalent Explosive



Adversaries will generally try and place a VBIED as close to the facility as possible in order to maximize its effect. If this is not done surreptitiously, or when vehicle barriers are in place to protect a prestige target, the adversary may attempt a ramming attack to defeat the barriers and get in closer proximity to the facility. The determination of a need for ramming is a function of the value of the target, the amount of setback, and the effective size of the device. However, a ramming attack is likely to include the suicide of the adversary, so the likelihood of this attack is mitigated somewhat by the lack of suicidal adversaries operating in the US. Examples of these events include the following:

7.20.7

- On June 9, 2009, a VBIED exploded at the Pearl Continental Hotel in Peshawar, Pakistan, killing at least 11 people and injuring at least 50 others. The Pearl Continental had implemented several protective measures prior to the attack, including large standoff distances and a vehicle inspection requirement for entering the premises.
- In 2005, a suicide driver smashed a VBIED packed with explosives through the Ayodha Temple Complex security gates in India.
- In developing plans for attacks against major financial institutions, Dhiren Barot recommended ramming tanker trucks into the lobbies of certain facilities as a potential tactic.^{lxv}

Curb weights for Jeep Grand Cherokee, Dodge Durango, Dodge Ram, and Nissan Pathfinder range from approximately 4300 to 5100 pounds. A 4700-pound vehicle with average acceleration is capable of achieving a speed of approximately 24 miles per hour from a standing start given a 100-foot acceleration distance. If the vehicle does not begin from a standing start (e.g., rounds a typical street corner and then begins its acceleration), it can achieve speeds approaching 30 miles per hour. If there is a downward slope of as little as two degrees, the achievable speed is 35 miles per hour.

Target Attractiveness

The unpredictable nature of the motivations of lone wolf adversaries makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary. However, Federal facilities, national monuments and icons, and highly symbolic commercial office buildings are all more likely to be targets for a VBIED attack and thus face a higher threat. Successful and even unsuccessful attacks against these targets provide terrorists with a potential media outlet to further their cause.

Although a facility may be hardened to prevent a terrorist from successfully attacking the facility with a VBIED, terrorists have demonstrated they will still attempt to attack these targets as displayed in the two East African U.S. Embassy bombings in 1998 and the 2008 attack on the U.S. Embassy in Sana'a, Syria and others. Where the target to be attacked is a prestige facility (e.g., seats of government, department headquarters, counter-terrorism facilities), larger VBIEDs tend to be deployed, often with suicide switching, and potentially in a ramming attack to penetrate a protected perimeter.

When tied to a VBIED attack, well-defended prestige targets (very high profile and symbolic facilities) with substantial standoff have a higher threat of this event.

Outlook

In assessing the likely size of a VBIED, analysts examined a TSWG study of over 200 incidents between January 2001 and December 2003. This information was compared against a State Department study conducted of 70 VBIEDs between 1982 and 1985. Both samples indicate that the anticipated size of a device has remained consistent over approximately 20 years. This trend is expected to remain fairly constant for the foreseeable future.

Terrorists have repeatedly shown their willingness and ability to use explosives as weapons worldwide and there is ample intelligence to support the conclusion that they will continue to use such devices to inflict harm. The threat of explosive attacks in the United States is of great concern considering terrorists' ability to make, obtain, and use explosives, the ready availability of components used in IED construction, the relative technological ease with which an IED can be fashioned, and the nature of our free society. Even while security measures are enhanced to counter the use of VBIEDs, their use in the U.S. is expected to increase in the future.

Based on experiences overseas, terrorists may shift from the tactic of one large VBIED, to a coordinated use of several smaller devices to gain access inside a secure perimeter and deploy a device close to a facility.

As more and more targets are hardened, it is expected that adversaries conducting VBIED attacks will seek softer targets which are still symbolically valuable. As those targets are hardened and particularly when setbacks are established that will reduce the effectiveness of a VBIED, ramming attacks may become part of the VBIED attack with some frequency. In prestige targets, sequential attacks, where the initial attack is intended to create a breach in barriers, allowing a follow-up attack within the protected perimeter, are anticipated in the future.

References

Vehicle Borne Improvised Explosive Devices in Worldwide Terrorism - A Contemporary Open Source Analysis, Technical Security Working Group, March 23, 2004

Federal Law Enforcement Training Center Counterterrorism Division, Introduction to Vehicle Borne Improvised Explosive Devices (VBIED), December 2004.

DHS/FBI, Potential Terrorist Attack Methods, April, 23, 2008

White House, National Strategy for Combating Terrorism, September 2006.

Homeland Security Council, National Strategy for Homeland Security, October 2007

US Department of Justice Media Release, Five Radical Islamists Convicted of Conspiring to Kill Soldiers at Fort Dix, December 22, 2008

US Army Training and Doctrine Command, Terror Operations: Case Studies in Terrorism, August 15, 2005

Federal Emergency Management Agency United States Fire Administration National Fire Data Center, the World Trade Center Bombing: Report and Analysis

FPS Information Bulletin HQ-IB-003-08, Recent Significant Terrorist Attacks against Infrastructure Targets, September 2008, September 22, 2008.

Memorial Institute for the Prevention of Terrorism - www.terrorisminfo.mipt.org, Terrorism Incidents and Significant Dates

Table 1-11: Number of U.S. Aircraft, Vehicles, Vessels, and Other Conveyances, Department of Transportation, Bureau of Statistics

Federal Register / Vol. 73, No. 251 / December 31, 2008

U.S. Army, TR-31-210 Improvised Munitions Manual, 1969


University of Maryland, Global Terrorism Database

ATF, Bomb Arson Tracking System (BATS)

U.S. District Court Middle District of Florida, Plea Agreement, US vs. Ahmed Mohamed, June 13, 2008.

Homeland Security Presidential Directive 19, Combating Terrorist Use of Explosives in the United States, February 2007

Overpressure curve calculated using A.T.-Blast version 2.2

Undesirable Event	7.21 Hostile Surveillance					
Definition	The surveillance of key assets, personnel, security features, operations, or sensitive areas from offsite, or outside secure areas for the purposes of collection of information in preparation for an attack.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Adversaries utilize the internet to obtain open source material on a potential target, and a team of 2 conducts surveillance from a nearby public location to observe specific operational details of the target in preparation for a possible attack.

Baseline Threat

Based on the number of adversary organizations seeking to carry out a variety of attacks on Federal facilities, and the demonstrated understanding that pre-operational surveillance is a definitive step in all successful attack planning, as well as for significant criminal enterprises, the baseline threat to Federal facilities from this event is assessed to be **HIGH**.

Analytical Basis

Surveillance of the target and the surrounding area is one of the most important elements of the terrorist planning effort. Their conduct typically is covert and can involve numerous collectors—either on foot or in vehicles—and also technological means that are more difficult to detect. Information detailing Al-Qa’ida surveillance of several U.S. locations demonstrates that the terrorist group has a sophisticated surveillance capacity and cases potential targets well in advance of an attack. Examples of these events include the following:

- An Al-Qa’ida training manual titled “Military Studies in the Jihad Against the Tyrants,” recovered in the United Kingdom in 2000 suggests that up to 80 percent of valuable information can be collected using public sources. In fact, much of the recently obtained surveillance information appears to come from the Internet, guide, or travel books, and the media.^{lxvi}
- In March 2005, a group calling itself the Media Jihad Brigade published a statement declaring its intent to wage “electronic jihad,” to include using the Internet to provide support to the Mujahidin on the ground. In an August 2005 Internet posting, an Islamic extremist group identified internet satellite mapping capabilities as “A Gift for the Mujahidin, a Program to Enable You to Watch the Cities of the World via Satellite.”^{lxvii}

- In 2004, Dhiren Barot, who conducted surveillance of several financial centers in the U.S., obtained much of the information contained in his planning reports from publicly available images and maps.

Employees were also cited as a source of information during the surveillance of one location. The training manual also suggests attending open houses or other ceremonies to obtain information about building interiors, which was done on at least one occasion.

Although the Internet allows for initial surveillance to take place in relative anonymity, actual “eyes-on” surveillance remains a critical aspect of pre-operational planning.^{lxviii} A manual detailing the kidnapping of Americans, for example, emphasized that the success of a previous kidnapping depended upon the attackers’ thorough knowledge of the target site. Operatives may be seen drawing, taking notes, or using cameras or video recording devices. These operatives may engage in routine activities at the surveillance location to avoid detection, such as purchasing a ticket, taking a tour, or mailing an item.^{lxix} Examples of these events include the following:

- In September 2009, the FBI disrupted plots to attack a Federal office building and courthouse in Springfield IL, and a commercial office tower in Dallas, TX, containing more than 200,000 square feet of government leased space. In both cases, the adversaries conducted surveillance on foot and in vehicles around the targets, as well as entering the facilities.
- On May 7, 2007, Mohamad Shnewer, Serdar Tatar and illegal alien brothers Dritan, Shain, and Eljvir Duka were arrested on charges related to their plans for a terrorist attack against Fort Dix. The suspects intended to acquire firearms and mount an attack against a concentration of soldiers on the post. The attack plan apparently called for a hit-and-run strike, with the suspects intending to escape afterward. The terrorist operatives used a nearby restaurant as cover for their surveillance. Recorded conversations revealed that Tatar delivered pizzas to Fort Dix from a pizzeria his family owned near the post. The six men showed interest in other East Coast military installations, but settled on Fort Dix largely because Tatar was familiar with the post.^{lxx}
- Three terrorists used overhead satellite images obtained from Google Earth in support of plans disrupted in 2007 to attack John F. Kennedy International Airport in New York. One of the terrorists worked as a cargo handler at the airport until he retired in 1995. In a recorded conversation, he confided to an FBI informant that his “unique knowledge of the airport” as a former cargo worker would help him launch a terrorist attack surpassing the magnitude of the 11 September 2001 attacks.
- The perpetrators of the London mass transit bombings rehearsed the attack on June 28, 2005 while on their respective routes in the London subway system. They wore backpacks during the dry run as they did when they executed the attack.
- In 2004, armed militants associated with the Chechen movement recruited construction workers familiar with the structure of a school in Beslan in North Ossetia, Russia, to place explosives under the floorboards in the school’s gym.^{lxxi}

- Seven members of a militia group were arrested in October 1996 in connection with a plot to bomb the FBI's fingerprint records facility in West Virginia. In planning for the attack, one member – a local firefighter – obtained confidential blue prints of the facility given to the fire department for pre-fire planning.

Target Attractiveness

The likelihood of being targeted for hostile surveillance correlates to the attractiveness as a target for specific threat events. Surveillance in preparation for an attack by terrorists and criminals alike is almost uniformly associated with successful attacks (other than spontaneous opportunistic events).

Facilities with higher-value assets, materials, information, etc. may face a higher threat from this type of event.


Outlook

It is expected that adversaries will continue to gather information and intelligence to identify targets and plan attacks against Federal facilities. As technology continues to improve and information becomes more widely available on the internet, adversaries will utilize open source information to the greatest extent possible in order to minimize the risk of detection. However, it is expected that at some point, all attack planning will still require in-person surveillance of the target.

Webcams at U.S. critical infrastructure locations, however, may allow the open observation of security measures, guard shift changes, and pedestrian and vehicular traffic patterns. An Islamic extremist website last year posted a link titled, "You Can Spy on the Enemies" that connected to a live webcam at a U. S. international airport. Airport authorities disabled the webcam after they were notified of the posting.^{lxxii}

References

See Section 7.32

Undesirable Event	7.22 Insider Threat					
Definition	Individuals with the access and/or inside knowledge of an organization that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Insider threat acts include a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance and sabotage. The coordination of an insider in perpetration of any other undesirable event is likely to lead to a greater chance at success.

Baseline Threat

A specific baseline threat for this event is not defined, as the threat level relates to the undesirable event the insider is supporting/perpetrating. The presence of a complicit, potentially disgruntled insider likely increases the threat of other undesirable events.

Analytical Basis

In most instances to date, the insider threat has been largely limited to primarily criminal acts of theft and espionage, with some evidence of sabotage.

Information from several recent planned or thwarted terrorist plots shows the importance of the use of insiders to gain access to targets and collect preoperational information. Examples of these events include the following:

- On May 7, 2007, six men were arrested on charges related to their plans for a terrorist attack against Fort Dix. The suspects intended to acquire firearms and mount an attack against a concentration of soldiers on the post. The attack plan apparently called for a hit-and-run strike, with the suspects intending to escape afterward. The group used a nearby restaurant as cover to gain access to the post for their surveillance.
- Russell Defreitas, the alleged mastermind behind the plot discovered in 2007 to explode jet fuel pipelines at John F. Kennedy (JFK) International Airport, had been a cargo handler at the airport. Defreitas worked as a cargo handler at the airport until he retired in 1995. In a recorded conversation Defreitas confided to an FBI informant that his “unique knowledge of the airport” as a former cargo worker, would help him launch a terrorist attack surpassing the magnitude of the 11 September 2001 attacks.

7.22.1

- In 2006 and 2007, Carol Ann Bond stole a quantity of 10-chloro-10H-phenoxarsine and potassium dichromate from her employer, a chemical manufacturer, and repeatedly attempted to use it to poison a former friend.
- Al-Qa'ida planner Dhiren Barot, whom UK authorities arrested in 2006, had tasked a member of his group to secure employment at a hotel in the United Kingdom to learn how to deactivate fire and security systems.
- In 2003, during a strike by contract employees at the USDA's Plum Island Animal Disease Research Center, infrastructure supporting the island was sabotaged by persons working on the island.

Target Attractiveness

Given the types of potential actors, there are corresponding motivations, which do not necessarily correlate to the characterization of the actor. Motivations for insiders can be summarized as some combination of: revenge for a perceived wrong; radicalization for advancement of religious or ideological objectives; or simple illicit financial gain.

Those who do commit malicious insider actions most commonly have a causal experience or mechanism to betrayal. These mechanisms or causations to malicious action can be categorized as coming from three different sources: 1) growing, exacerbated or unaddressed discontent with their place or value in the organization; 2) recruitment by hostile outside entities or groups; or 3) infiltration of a malicious actor to a trusted position on an infrastructure operator's staff.

Outlook

The insider threat will continue to pose a significant challenge to disrupting adversary acts in the future. Rapidly escalating technology and network risks are combining with growing globalization of workforces, supply chains, and service providers to produce new threats and risks.

References

JHSA - Recent Terrorist Plots Highlight Insider Threat, 7 August 2007

The National Infrastructure Advisory Council Final Report and Recommendations on the Insider Threat to Critical Infrastructures, April 28, 2008

Undesirable Event	7.23 Kidnapping					
Definition	The abduction of an occupant or visitor from a facility, including inside secured areas (e.g., a child care center) or outside on the site (e.g., a Government-controlled parking lot).					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Two adversaries with handguns attempt to abduct a senior Federal employee from a parking area.

- OR -

In facilities with a child care center, an unarmed non-custodial parent attempts to enter a controlled area and abduct a child.

Baseline Threat

Based on the frequency of historical events, terrorism literature describing operational planning requirements, and disrupted plots, the baseline threat of an abduction of employees and officials at Federal facilities is assessed to be **LOW**.

Based on the frequency of historical events in general, the baseline threat of an abduction of a child at Federal facilities is assessed to be **MODERATE**.

Analytical Basis

Kidnapping and hostage-taking are tactics used by terrorist groups, criminals, and other individuals all over the world. Terrorists utilize kidnappings and hostage-taking in order to provoke a reaction in a targeted group through the threat of harm to the kidnapped individual or group. Traditionally, terrorists seek to leverage their victims for money, military equipment, and release of prisoners, media attention, or other specific actions from a country's government. Examples of these events include the following:

- On September 24, 2009, the FBI made an arrest of a U.S. citizen which disrupted a plot to utilize a car bomb against the Paul Findley U.S. Federal Building and Courthouse in Springfield, IL. During meetings with undercover agents, the adversary suggested a possible plan to abduct a Senator while posing as an FBI agent.
- On June 14, 2009, nine foreigners, including three children, were kidnapped by Shiite rebels in northern Yemen. The foreigners were working at a hospital in the region. Houthi rebels are Shiite militants who have been fighting the government for years. The militants were hoping to derail the peace and reconstruction process in Saada.^{lxxiii}

7.23.1

- In June 2006, the Canadian Government uncovered an alleged terrorist plot to storm the Ottawa Parliament, hold politicians hostage, and demand the release of Muslim prisoners from Canadian jails and the withdrawal of Canadian military forces from Afghanistan.

Kidnapping of government officials inside the U.S. is a rare occurrence, but attempts have been made in the past. For example, on December 7 1981, James W. Von Brunn attempted to kidnap 6 members of the Federal Reserve Board from their headquarters in Washington, D.C. Von Brunn was reportedly angry over interest rates. In 2009, Von Brunn attacked the National Holocaust Museum, in Washington, DC, killing a security guard.

In a terrorist training document obtained from online sources, terrorists are instructed to seek out a lone adult male with some significant status at work, and abduct him from an isolated location, way from sensitive areas and areas which are routinely patrolled. The location will also ideally have more than one entrance and exit. The document lays out extensive step-by-step instructions for identifying targets, carrying out the abduction, hiding the victim, negotiations, security of the operation, etc.^{lxxiv}

According to the National Crime Information Center, in 2008, 20,562 of 778,161 missing persons reported were listed as “missing involuntarily.” This included 6,094 (29 percent) under the age of 18. In 2007, 21,747 of 814,957 missing persons were reported as “missing involuntarily,” of which 6,165 (28 percent) were under the age of 18.

Kidnapping makes up less than two percent of all violent crimes against juveniles reported to police. Based on the identity of the perpetrator, there are three distinct types of kidnapping: kidnapping by a relative of the victim or “family kidnapping” (49 percent), kidnapping by an acquaintance of the victim or “acquaintance kidnapping” (27 percent), and kidnapping by a stranger to the victim or “stranger kidnapping” (24 percent). According to DOJ statistics, in 1999 there were an estimated 58,200 child victims of nonfamily abduction, and 117,200 were victims of family abduction. Only 115 incidents of the “stereotypical” stranger abduction were reported.^{lxxv}

Family kidnapping is committed primarily by parents, it involves a larger percentage of female perpetrators (43 percent) than other types of kidnapping offenses, occurs more frequently to children under six, equally victimizes juveniles of both sexes, and most often originates in the home. Schools are an unusual site for abduction, even family abduction (only five percent of family, four percent of acquaintance, and three percent of stranger kidnappings occur at school).^{lxxvi} Family abductions are most commonly carried out by only one perpetrator.^{lxxvii} Examples of these events include the following:

- In June 2008, a child was abducted from a private child care center in Arkansas by a woman who called the center, then arrived claiming there was a family emergency. He was reunited with his parents that night and the abductor was arrested.
- In April 2008, an employee of a child care center in Houston, TX kidnapped a child from the private center. The employee was a new trainee. Police suspected she had obtained the job at the center for the sole purpose of abducting the child. The child was later reunited with her parents later that day and the abductor arrested.

Since the logistics of kidnapping or hostage-taking are fairly complicated with regard to the initial abduction, kidnappers will often work in groups. A high-value kidnapping target, in particular, likely necessitates a significant amount of planning and surveillance. However, family abductions of children are far more likely to be carried out by only one perpetrator.^{lxxviii}

In the case of family kidnapping incidents, only one percent involved use of a weapon, and only seven percent involved any use of force.^{lxxix}

Target Attractiveness

In facilities with child care centers and high-profile officials, the threat of kidnapping is estimated to be higher.


Outlook

The rate of criminally-motivated kidnapping is expected to remain constant for the foreseeable future. Kidnapping by drug and human smuggling organizations is also becoming popular in the Southwestern US along the southern border.^{lxxx}

Incidences of stereotypical child abduction do not appear to be on the rise, and thus the trend is expected to remain relatively stable in the foreseeable future.

References

See Section 7.32

Undesirable Event	7.24 Release of Onsite Hazardous Materials					
Definition	Unauthorized access to hazardous materials stored onsite with the intent to release/disburse such materials to harm personnel or damage the facility.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	YES	Classification	S	Date	10-16-09	

Design-Basis Threat Scenario

An adversary accesses external storage tanks of hazardous materials and manipulates valves or connections to create a leak.

Baseline Threat

Based on the limited locations where hazardous materials are stored at Federal facilities, the unavailability of information to an adversary, and the lack of historical frequency, the baseline threat to Federal facilities from this event are assessed to be **MODERATE**.

- OR -

The release of a small amount of hazardous material, such as cleaning or other types of general use chemicals, the baseline threat to Federal facilities from this type of event is also assessed to be **MODERATE**.

Analytical Basis

Hazardous materials are substances that are combustible, explosive, flammable, corrosive, toxic, noxious, oxidizable, an irritant, or radioactive. A hazardous material spill or release can pose a risk to life, health, property, or the environment. An incident can result in the evacuation of a few people, a section of a facility, or an entire neighborhood. Most major chemical releases can occur anywhere at any time. Examples of these events include the following:

- In November 2005, several high pressure containers of arsine and chlorine were tampered with at a research facility in Palo Alto, CA. The metal couplings were unscrewed. There was no apparent attempt to remove the containers from the facility, and it is not known whether the facility was broken into or if the tampering was conducted by an insider.^{lxxxix}
- In April 1997, four Ku Klux Klan members were caught planning to blow up a natural gas refinery outside Bridgeport, Texas. The suspects planned to place pipe bombs around storage tanks they believed to contain hydrogen sulfide to cause the release of a toxic cloud. The explosion was to have been a diversion for their main act, the robbery of an armored car 9 miles away. Police say the Klansmen intended to use the money to finance other terrorist acts.^{lxxxii}

7.24.1

On the basis of Al-Qa'ida's and other terrorists' expressed goals, the DHS Office of Intelligence and Analysis (I&A) and the FBI have assessed with medium confidence that the most likely terrorist objective in attacking chemical infrastructure would be the release of toxic industrial chemicals to cause large numbers of casualties.^{lxxxiii}

Target Attractiveness


Research and development laboratories, processing plants with associated chemicals, or similar facilities which store significant quantities of hazardous materials – including chemical, biological, radiological, and nuclear – may face a higher threat to this event. Such facilities which are located in areas with a large population in close proximity may face an even higher threat. Government labs which carry out research involving CBRN materials often become the subject of media attention, which can highlight them as potential targets for adversaries.

Outlook

The storage of large quantities of hazardous materials at government facilities is not a frequent or widely known practice and is not expected to become so.

References

See Section 7.32

Undesirable Event	7.25 Robbery					
Definition	Unauthorized taking of Government-owned or personal property from an employee or other person(s) by force or threat of force. The incident could occur inside or outside of a facility.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Single assailant armed with a semi-automatic handgun confronts an employee at a cash window (or similar disbursement location where valuables are stored).

- OR -

Single assailant armed with a knife confronts an employee approaching his vehicle in the rear parking lot of the facility.

Baseline Threat

Based on nationwide crime statistics and the frequency of events at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **LOW**. Crime rates vary significantly from location to location, and should be considered when characterizing this threat at a specific facility.

Analytical Basis

Robbery is a relatively simple act. Planning and preparation may increase the likelihood of complete success or decrease the probability of detection.

In 2007, 445,125 robberies were reported through the FBI's Uniform Crime Reporting (UCR) program. This did represent a decrease from the number of crimes reported in 2006. Between 1988 and 2007, robbery made up approximately 32 percent of all violent crime.^{lxxxiv}

Robberies per 100,000 Inhabitants (2007) ^{lxxxv}		
Population	Offenses known	Rate
Cities of 1,000,000 and over	94,385	374.2
Cities of 500,000 to 999,999	61,177	382.1
Cities of 250,000 to 499,999	42,859	337.0
Cities of 100,000 to 249,999	63,376	226.5
Cities of 50,000 to 99,999	45,208	153.1
Cities of 25,000 to 49,999	27,957	111.2
Cities of 10,000 to 24,999	20,306	80.1
Cities of under 10,000	11,694	56.1
Metropolitan Counties	50,286	79.7

Non-metropolitan Counties ¹	4,038	16.4
Suburban Areas ²	90,648	80.1

¹ Includes state police agencies that report aggregately for the entire state.

² Suburban areas include law enforcement agencies in cities with less than 50,000 inhabitants and county law enforcement agencies that are within a Metropolitan Statistical Area. Suburban area excludes all metropolitan agencies associated with a principal city. The agencies associated with suburban areas also appear in other groups within this table.

In 2007, approximately 43 percent of all robberies reported involved use of a firearm; 40 percent involved no weapons (strong arm); 8 percent involved use of an edged weapon; and, 9 percent involved other weapons.^{lxxxvi}

The Department of Homeland Security's Federal Protective Service (FPS) records statistics on criminal activity in approximately 8800 General Services Administration (GSA) facilities. In 2007, FPS reports there were 18 robberies in GSA facilities; in 2008 there were nine.

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI's Uniform Crime Reporting (UCR) Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Target Attractiveness

Random robberies may be related to the location of the facility. Facilities in high-crime areas are more likely to face threats of robbery and similar violent crime perpetrated against employees and visitors, generally as they approach or depart the facility. Approximately 70 percent of robberies take place on the street, at residences, banks, convenience stores, and gas stations. Only 30 percent take place at other locations, including commercial businesses.

Robbery in federal facilities is generally related to the nature of the work and may take place inside the facility itself or on the grounds. Facilities with high amounts of public contact, missions that are adversarial or controversial in nature and cash disbursement or collection operations are more likely to be subject to robbery attempts.

Facilities with higher-value assets, materials, information, etc. may face a higher threat from this type of event.

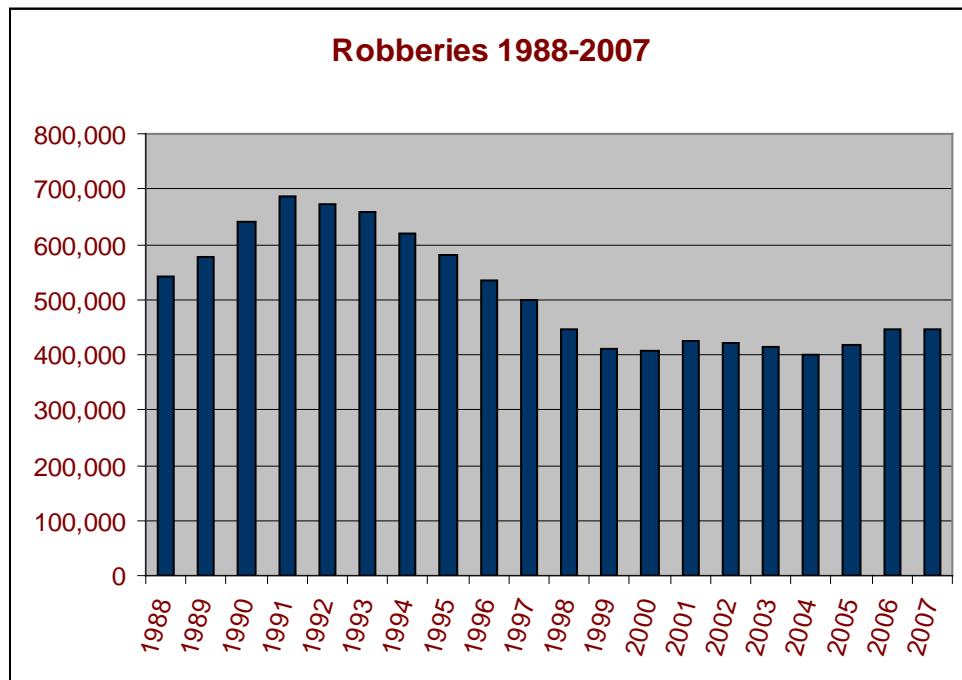
Locations with remote parking lots, proximity to high crime or neglected neighborhoods, areas frequented by transients, etc., present a higher threat environment.

Outlook

After a peak in violent crime of about 1.9 million reported offenses in 1993, the nation has seen a reduction to approximately 1.4 million crimes, a rate that has remained fairly steady since 1999.


According to FBI statistics, violent crime overall is down 8.2 percent nationally from 1998 to 2007, with robberies down less than 1 percent in that 10-year period. Robberies decreased slightly from 2006 to 2007.^{lxxxvii}

This trend is expected to stay relatively constant for the foreseeable future. However, local crime rates vary, even from neighborhood to neighborhood.



References

See Section 7.32

Undesirable Event	7.26 Theft					
Definition	Unauthorized removal of Government-owned or personal property from a facility.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Single perpetrator authorized to have access, using stealth to obtain and conceal the property while removing it from the facility.

Baseline Threat

Based on nationwide crime statistics and the frequency of events at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **VERY HIGH**. Crime rates vary significantly from location to location, and should be considered when characterizing this threat at a specific facility.

Analytical Basis

In 2007, 6,568,572 thefts were reported through the FBI's UCR program, totaling \$8,562,210,003 (not including motor vehicles). This did represent a decrease from the number of crimes reported in 2006. Between 1988 and 2007, theft made up approximately 66 percent of all property crime; ahead of burglary (22 percent) and motor vehicle theft (12 percent).^{lxxxviii}

Thefts by Type (2007)		
Pocket-picking	27,408	0.4 %
Purse-snatching	38,058	0.6 %
Shoplifting	978,978	14.9 %
From motor vehicles	1,706,979	26.0 %
Motor vehicle accessories	599,063	9.1 %
Bicycles	224,345	3.4 %
From buildings	789,123	12.0 %
From coin-operated machines	31,036	0.5 %
All others	2,173,581	33.1 %

Thefts by Value (2007)		
Over \$200	2,884,126	37.6 %
\$50 to \$200	1,471,078	19.2 %
Under \$50	2,213,368	28.9 %
Motor vehicle theft	1,095,769	14.3 %

Of thefts in 2007, only approximately 12 percent were from buildings, with another 26 percent from motor vehicles. Approximately 29 percent of stolen property was recovered.

The Department of Homeland Security's FPS records statistics on criminal activity in approximately 8800 GSA facilities. In 2007, FPS reports there were 1840 thefts in GSA facilities; in 2008 there were 1465. FPS also reports 94 auto thefts in 2007 and 46 in 2008.

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI's Uniform Crime Reporting (UCR) Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Target Attractiveness

Theft of tangible property is generally a relatively unsophisticated crime of opportunity, and requires very little planning or preparation to be successful. Random criminal actions, particularly thefts from vehicles or pick-pocketing and purse-snatching may be related to the location of the facility. Facilities in high-crime areas are more likely to face threats of this nature perpetrated against employees and visitors, generally as they approach or depart the facility.

Greater emphasis on planning and preparation may increase the likelihood of complete success, decrease the probability of detection, and be employed against a higher-value asset.

Facilities with higher-value assets, materials, information, etc. may face a higher threat from this type of event.

Often the perpetrator is another occupant who is able to gain access to the property through casual means. Internal thefts, perpetrated by persons with authorized access (including authorized visitors) are also often crimes of opportunity. Of particular risk are unsecured office spaces, especially systems furniture (cubicle) environments where security of the space cannot be achieved.

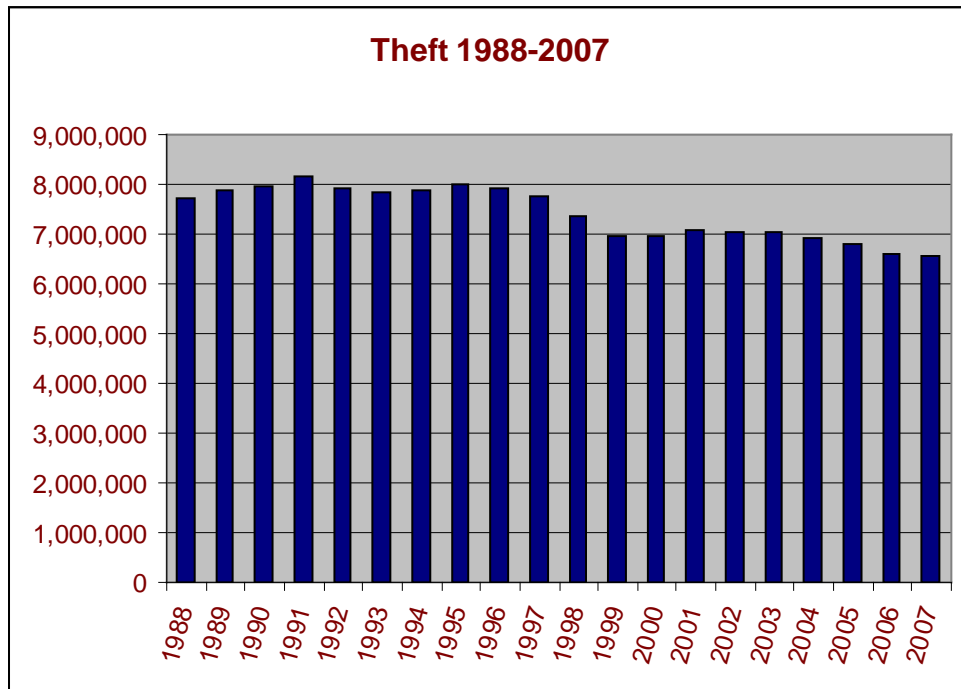
Locations with remote parking lots, proximity to high crime or neglected neighborhoods, areas frequented by transients, etc., present a higher threat environment for theft from vehicles.

Outlook

After a peak in larceny-theft of about 8.1 million reported offenses in 1991, the nation has seen a reduction to below 7 million crimes, a rate that has continued to decline since 2003.


According to FBI statistics, property crime overall is down 10 percent nationally from 1998 to 2007, with larceny-theft down 11 percent in that 10-year period. Property crime in all categories decreased from 2006 to 2007.^{lxxxix}

This trend is expected to continue a slow decline for the foreseeable future. However, local crime rates vary, even from neighborhood to neighborhood.



References

See Section 7.32

Undesirable Event	7.27 Unauthorized Entry - Forced						
Definition	Unauthorized access to a facility or controlled area by forced entry.						
Original Assessment	12-17-09	Revision	0	Date	N		
Classified Annex	No	Classification		Date			

Design-Basis Threat Scenario

Two adversaries equipped with hand tools, including crowbars, hammers, channel locks, vise grips, and screwdrivers.

Baseline Threat

Based on the unsophisticated nature of the event, nationwide crime statistics, and the frequency of events at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **HIGH**. Crime rates vary significantly from location to location, and should be considered when characterizing this threat at a specific facility.

Analytical Basis

Burglary is often a relatively unsophisticated crime, and requires very little planning or preparation to be successful. It is often a crime of opportunity when doors or windows are unlocked, and no force is necessary.

In 2007, 2,179,140 burglaries were reported through the FBI's UCR program. This represented a slight decrease from the number of burglaries reported in 2006. Burglary accounted for approximately 22 percent of all property crime committed in 2007.^{xc}

Burglaries per 100,000 Inhabitants (2007) ^{xc}		
Population	Offenses known	Rate
Cities of 1,000,000 and over	187,272	742.5
Cities of 500,000 to 999,999	188,743	1,178.7
Cities of 250,000 to 499,999	135,841	1,068.2
Cities of 100,000 to 249,999	262,786	939.1
Cities of 50,000 to 99,999	227,456	770.5
Cities of 25,000 to 49,999	168,866	671.5
Cities of 10,000 to 24,999	159,940	630.5
Cities of under 10,000	133,839	642.4
Metropolitan Counties	390,058	618.2
Non-metropolitan Counties *	132,800	539.7
Suburban Areas **	672,268	594.4

7.27.1

** Includes state police agencies that report aggregately for the entire state*

*** Suburban areas include law enforcement agencies in cities with less than 50,000 inhabitants and county law enforcement agencies that are within a Metropolitan Statistical Area. Suburban area excludes all metropolitan agencies associated with a principal city. The agencies associated with suburban areas also appear in other groups within this table.*

Only 32 percent of all burglaries were of non-residential buildings, including stores, office buildings, etc. Of these, 42 percent were known to have taken place at night, 32 percent during the day, and 26 percent the time could not be determined. Approximately 61 percent involved forcible entry, 32 percent were without force, and 7 percent were forcible entry attempts.

The Department of Homeland Security's Federal Protective Service (FPS) records statistics on criminal activity in approximately 8800 General Services Administration (GSA) facilities. In 2007, FPS reports there were 86 burglaries of GSA facilities; in 2008 there were 63. Examples of these events include the following:

- In March 2009, unknown person(s) broke into a second floor window in a U.S. Federal Labor Relations Authority office and stole 3 laptop computers. The adversaries used nearby scaffolding to access the window.
- In June 2008, unknown person(s) threw a boulder through a double pane window of the Social Security Administration Office in Phoenix, AZ. They were able to access the room and steal a camera and tripod. The area was alarmed however; there was no alarm activation at the Security Company or local police department. The exterior camera covering the area was reported as being distorted with no recording.
- Also in June 2008, unknown person(s) broke into interior offices of the U.S. Citizenship & Immigration Services facility located in Arlington, VA. Nine laptop computers were stolen. Investigation revealed eight of the laptop computers were secured in two separate file cabinets and both were broken into. Also both office doors were forced open by what appeared to be a screwdriver or flat tipped tool.
- A man was arrested at the Federal building in Salt Lake City, UT, in July 1989 after attempting to break into an FBI office by prying on an interior suite door and throwing a fire extinguisher against a window. The window did not break. A search of the building showed that offices of the Department of the Interior may also have been burglarized. The adversary gained access by using a brick to break out a basement window.

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI's UCR Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Target Attractiveness

Random burglaries may be related to the location of the facility. Facilities in high-crime areas are more likely to face threats of burglary and similar property crimes. Facilities which are in remote locations and not staffed after hours are more likely to be targeted than those in highly populated areas or with around-the-clock staffing. Additionally, in lightly or unpopulated locations, adversaries are likely to be willing to spend more time attempting to force entry.

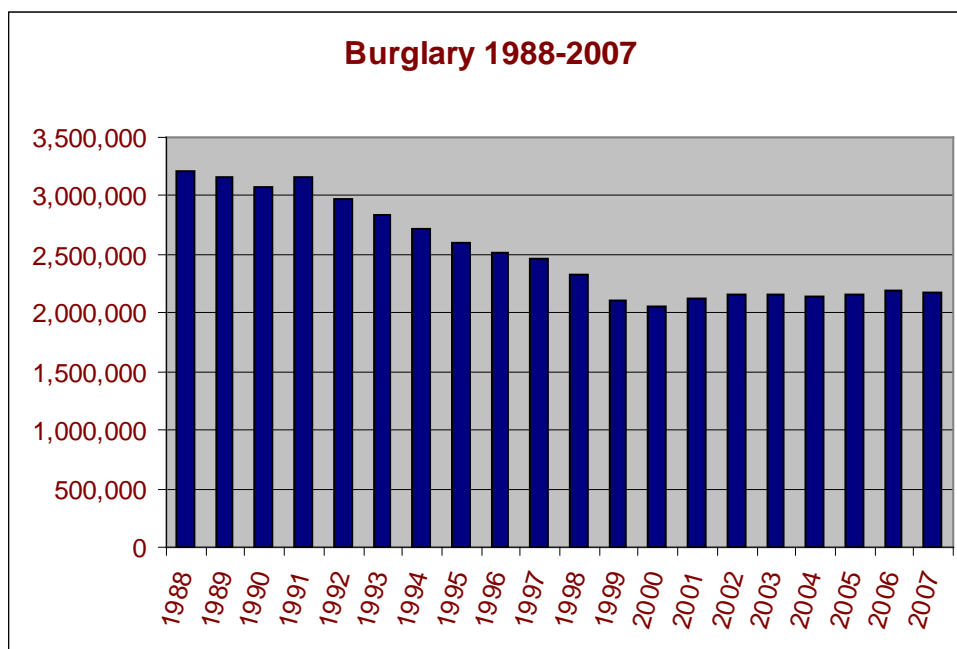
The amount of force or complexity be used to gain entry will increase, as the value of the targeted asset increases. Greater emphasis on planning and preparation may be associated with higher value assets, increase the likelihood of complete success, or decrease the probability of detection during or after the fact.

Burglary in federal facilities is most often related to general theft of assets, such as computers or other valuable office equipment. However, facilities which store quantities of sensitive or classified information may be targeted specifically for that information. In this case, a larger team of adversaries may be faced, the adversaries are likely to be more highly motivated, better equipped, and perpetrate the act in such a manner as to minimize the chance of detection.

Outlook


After a peak in property crime of almost 13 million reported offenses in 1991, the nation has seen a reduction to approximately 10 million crimes, a rate that has steadily declined since 2002.

According to FBI statistics, property crime overall is down 10.1 percent nationally from 1998 to 2007, with burglaries down approximately 6 percent in that 10-year period. Burglaries decreased slightly from 2006 to 2007.^{xcii} This trend is expected to stay relatively constant for the foreseeable future. However, local crime rates vary, even from neighborhood to neighborhood.



References

See Section 7.32

Undesirable Event	7.28 Unauthorized Entry - Surreptitious					
Definition	Unauthorized access to a facility or controlled area by stealth.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

A single adversary gains entry to a facility through an unsecured door or window. The adversary is capable of accessing a second story window or one-story roof by using available means to climb.

Baseline Threat

Based on nationwide crime statistics and the frequency of events at Federal facilities, and the trend away from surreptitious entry as a tactic of espionage, the baseline threat to Federal facilities from this event is assessed to be **MODERATE**. Crime rates vary significantly from location to location, and should be considered when characterizing this threat at a specific facility.

Analytical Basis

Burglary is often a relatively unsophisticated crime, and requires very little planning or preparation to be successful, particularly if no force is used. It is often a crime of opportunity when doors or windows are unlocked, and no force is necessary.

In 2007, 2,179,140 burglaries were reported were reported through the FBI's UCR program. This did represent a slight decrease from the number of burglaries reported in 2006. Burglary accounted for approximately 22 percent of all property crime committed in 2007.^{xciii}

Burglaries per 100,000 Inhabitants (2007)^{xciv}		
Population	Offenses known	Rate
Cities of 1,000,000 and over	187,272	742.5
Cities of 500,000 to 999,999	188,743	1,178.7
Cities of 250,000 to 499,999	135,841	1,068.2
Cities of 100,000 to 249,999	262,786	939.1
Cities of 50,000 to 99,999	227,456	770.5
Cities of 25,000 to 49,999	168,866	671.5
Cities of 10,000 to 24,999	159,940	630.5
Cities of under 10,000	133,839	642.4
Metropolitan Counties	390,058	618.2
Non-metropolitan Counties *	132,800	539.7
Suburban Areas **	672,268	594.4

* Includes state police agencies that report aggregately for the entire state.

***Suburban areas include law enforcement agencies in cities with less than 50,000 inhabitants and county law enforcement agencies that are within a Metropolitan Statistical Area. Suburban area excludes all metropolitan agencies associated with a principal city. The agencies associated with suburban areas also appear in other groups within this table.*

Only 32 percent of all burglaries were of non-residential buildings, including stores, office buildings, etc. Of these, 42 percent were known to have taken place at night, 32 percent during the day, and 26 percent the time could not be determined. Approximately 32 percent were without force, 61 percent involved forcible entry, and 7 percent were forcible entry attempts.

An example of such an event took place in 2007 when a physical breach of security resulted in the theft of data center hardware in Chicago. The robbers used a hook to lower an old-fashioned fire escape on the side of the building in order to gain access surreptitiously at night. A guard from a security company wasn't at his post, the robbers waited in a hall for the lone employee who was on duty at the time to leave the data center. Once the robbers accosted and subdued the worker, they swiped his employee badge through a scanner and entered his security PIN code on a keypad outside the door to the data center. The security system then prompted them for a fingerprint scan, which the employee was forced to do, according to Faulkner. The robbers stole servers and networking equipment that belonged to a collocation customer and that Faulkner estimated would cost between \$50,000 and \$100,000 if bought new. ^{xcv}

The Department of Homeland Security's Federal Protective Service (FPS) records statistics on criminal activity in approximately 8800 General Services Administration (GSA) facilities. In 2007, FPS reports there were 86 burglaries of GSA facilities; in 2008 there were 63.

An example of such a scenario took place in February 2002 when a woman burglarized a Federal Highway Administration building in Lakewood, Colorado. She stole a number of computers which contained sensitive information on the Hoover Dam.

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI's UCR Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Surreptitious entry is also often a tactic used in espionage incidents, where a goal is to obtain classified or proprietary information without the knowledge that it has been compromised. However, espionage tradecraft has turned more to the use of the insider and technological means rather than surreptitious entries.

Target Attractiveness

Random burglaries may be related to the location of the facility. Facilities in high-crime areas are more likely to face threats of burglary and similar property crimes. Facilities which are in remote locations and not staffed after hours are more likely to be targeted than those in highly populated areas or with around-the-clock staffing. Additionally, in lightly or unpopulated locations, adversaries are likely to be willing to spend more time attempting to force entry.

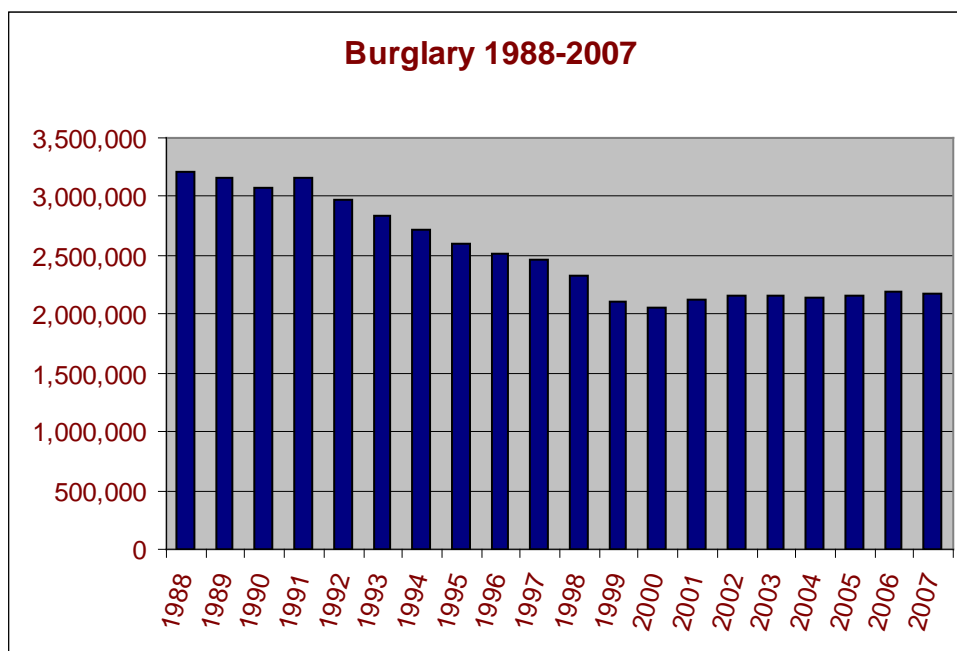
As the value of the targeted asset increases, so too may the amount of force that will be used by an adversary to gain entry to a facility. Greater emphasis on planning and preparation may be associated with higher value assets, increase the likelihood of complete success, or decrease the probability of detection during or after the fact.

Burglary in federal facilities is most often related to general theft of assets, such as computers or other valuable office equipment. However, facilities which store quantities of sensitive or classified information may be targeted specifically for that information. In this case, a larger team of adversaries may be faced, the adversaries are likely to be more highly motivated, better equipped, and perpetrate the act in such a manner as to minimize the chance of detection.

Outlook


After a peak in property crime of almost 13 million reported offenses in 1991, the nation has seen a reduction to approximately 10 million crimes, a rate that has steadily declined since 2002.

According to FBI statistics, property crime overall is down 10.1 percent nationally from 1998 to 2007, with burglaries down approximately 6 percent in that 10-year period. Burglaries decreased slightly from 2006 to 2007.^{xvii} This trend is expected to stay relatively constant for the foreseeable future. However, local crime rates vary, even from neighborhood to neighborhood.



References

See Section 7.32

Undesirable Event	7.29 Vandalism					
Definition	Destruction, damage, or defacing of Government-owned or personal property or assets.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

Unknown adversaries painted graffiti on facility walls or external assets.

Baseline Threat

Based on nationwide crime statistics, presence of adversary groups who commonly use this as a tactic against Federal facilities, and the frequency of random and directed events at Federal facilities, the baseline threat to Federal facilities from this event is assessed to be **HIGH**. Crime rates vary significantly from location to location, and should be considered when characterizing this threat at a specific facility.

Analytical Basis

Vandalism is often associated with juveniles and gangs, but is also a tactic used by typically nonviolent adversary organizations. When associated with an adversary group, it is often used to make a political statement.

In 2007, 221,040 persons were arrested for vandalism. That represents a slight increase from the number of arrests reported in 2006. Approximately 38 percent of those arrested in 2007 were under the age of 18.

Vandalism per 100,000 Inhabitants (2007)		
Population	Offenses known	Rate
Cities of 250,000 and over	44,359	106.9
Cities of 100,000 to 249,999	25,076	112.3
Cities of 50,000 to 99,999	30,065	111.2
Cities of 25,000 to 49,999	25,749	109.1
Cities of 10,000 to 24,999	26,205	111.3
Cities of under 10,000	26,262	135.3
Metropolitan Counties	30,259	63.9
Non-metropolitan Counties *	13,065	63.0
Suburban Areas **	85,621	86.5

* Includes state police agencies that report aggregately for the entire state.

**Suburban areas include law enforcement agencies in cities with less than 50,000 inhabitants and county law enforcement agencies that are within a Metropolitan Statistical Area. Suburban area excludes all metropolitan agencies associated with a principal city. The agencies associated with suburban areas also appear in other groups within this table.

The National Crime Prevention Council reports that graffiti is the most common form of vandalism. Approximately 80 percent of graffiti is gang or “tagger” related.

The Department of Homeland Security’s Federal Protective Service (FPS) records statistics on criminal activity in approximately 8800 General Services Administration (GSA) facilities. In 2007, FPS reports there were 600 acts of vandalism at GSA facilities; in 2008 there were 494.

An example of this event took place in July 2000 when several government-owned vehicles were vandalized and approximately 500 trees were destroyed during an attack against a U.S. Forest Service research facility in Wisconsin. The attack was carried out by members of the Earth Liberation Front (ELF), the most active environmental extremist movement in the United States. ELF targeted the facility because they mistakenly believed that scientists there were genetically engineering trees, according to court materials. The vehicles defaced featured multiple references to ELF, including “ELF is watching the U.S. Forest Service.” ELF claimed responsibility for the incident in a communiqué released shortly afterwards; the statement described the attack as a response to bioengineering. SOURCE: Anti-Defamation League

For more information regarding crime statistics in particular geographic locations, contact local law enforcement or visit the FBI’s UCR Program website, at <http://www.fbi.gov/ucr/ucr.htm>.

Target Attractiveness

Vandalism is a relatively unsophisticated crime, and requires very little planning or preparation to be successful. It is often opportunistic. Greater emphasis on planning and preparation may increase the extent of damage or decrease the probability of detection.

Facilities with higher-value assets, materials, information, etc may face a higher threat from this type of event.

Random acts of vandalism may be related to the location of the facility. Facilities in high-crime areas are more likely to be subject to random damage or destruction of property, generally along public paths of travel around the facility. Additionally, facilities in areas where gang activity is high may be subject to “tagging” by gang members.

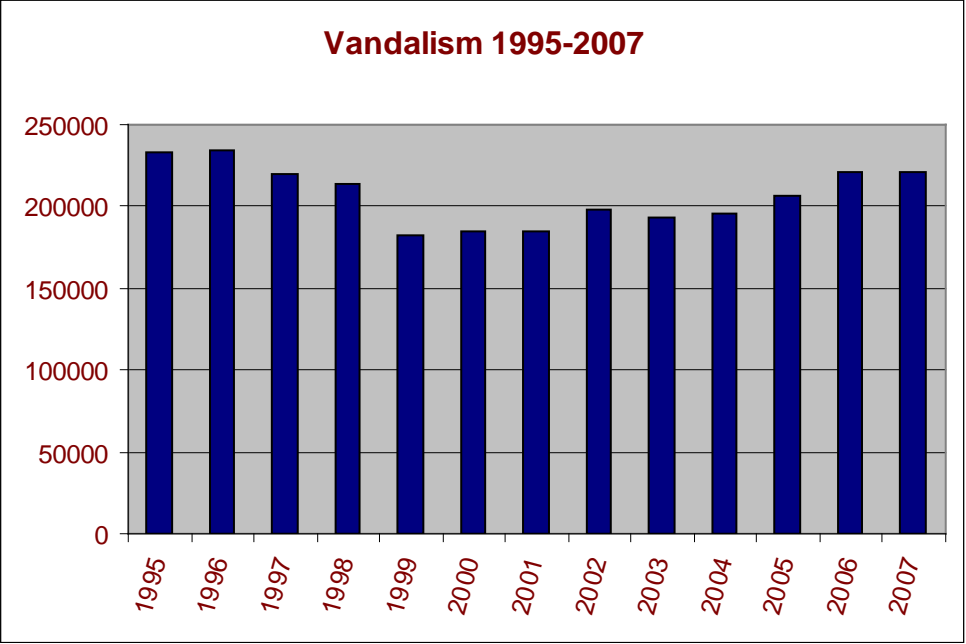
Vandalism directed at specific agencies is often related to controversial missions. Vandalism is a frequent tactic used by special interest extremist groups to express beliefs about the nature of operations at a facility. Facilities with missions associated with environmental actions, use of public land, and controversial research and development, particularly where animals are involved, may be more likely targets of vandalism.

Outlook

According to FBI statistics, property crime overall is down 10 percent nationally from 1998 to 2007, with vandalism arrests down approximately 3 percent in that 10-year period.^{xcvii} Vandalism dipped from a peak in 1996 to a low in 1999, but has maintained a fairly steady increase since 1999.^{xcviii}


This trend is expected to stay relatively constant or increase slightly for the foreseeable future. However, local crime rates vary, even from neighborhood to neighborhood.

7.29.2



References

See Section 7.32

Undesirable Event	7.30 Vehicle Ramming					
Definition	Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock) or breach a defined perimeter.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Design-Basis Threat Scenario

A 4700-pound pickup or sport utility vehicle (SUV) traveling at 35 miles per hour attempts to ram into a facility.

Baseline Threat

Based on the historical frequency of the event, the baseline threat to Federal facilities when the vehicle is used as the weapon is assessed to be **MODERATE**.

Analytical Basis

The use of the vehicle as a weapon itself is a frequent tactic. The intent may be to cause property damage, injure or kill building occupants, commit suicide, or to simply make a statement by committing the act, without regard to the consequences. In these instances, the adversary is usually experiencing an extreme state of emotional duress, discontentment, or dissatisfaction with an immediate situation. Examples of these events include the following:

- In August 2008, a 48-year old man rammed his SUV into an Internal Revenue Service building in Birmingham, Alabama. The 48-year-old man was apparently distraught over finances, and had made a threat against an IRS agent and later threatened to take his own life. His SUV's bumper breached two of the lower office windows.
- In June 2007, two men rammed a flaming SUV into the main terminal at Glasgow Airport in Scotland.
- In April 2006, Roy Thomas Chaivarlis drove his 1988 Dodge delivery van across the front lawn of a state police station in Kittanning, PA, striking the building and causing the partial collapse of the front wall and door. Chaivarlis later told investigators that he hated the state police. The vehicle traveled about 10 feet into the lobby.

- On the afternoon of March 3, 2006, Mohammed Reza Taheri-azar, a U.S. citizen born in Iran, drove a rented Jeep Grand Cherokee through a common courtyard area of the University of North Carolina, injuring nine people. After the attack, Taheri-Azar claimed he was following God in avenging the U.S. government's killing of Muslims around the world. While not readily accessible to vehicular traffic beyond a narrow service road, the barricades that normally prevent cars from approaching the courtyard area were not in place on the day of the attack.
- In May 2002, a Winston-Salem man reported to have a 2-year-old grudge against the Kernersville News rammed his truck through the front of the newspaper building located in Kernersville, NC.

Curb weights for 2009 model year Jeep Grand Cherokee, Dodge Durango, Dodge Ram, and Nissan Pathfinder range from approximately 4300 to 5100 pounds. A 4700-pound vehicle with average acceleration is capable of achieving a speed of approximately 24 miles per hour from a standing start given a 100-foot acceleration distance. If the vehicle does not begin from a standing start (e.g., rounds a typical street corner and then begins its acceleration), it can achieve speeds approaching 30 miles per hour. If there is a downward slope of as little as 2 degrees, the achievable speed is 35 miles per hour.

Target Attractiveness

Using a vehicle to deliberately ram a facility is an infrequent event. However, when a ramming does occur, it typically involves a single individual attempting to resolve a perceived injustice. The unpredictable nature of the motivations of lone wolf adversaries, or persons reacting to a singular event in an emotionally charged state of mind, makes it difficult to determine what specific factors will make a facility or individual a more attractive target to a lone wolf adversary. A ramming may not be so much directed at a specific individual as much as an entire agency. Conversely, the attack may be aimed at a specific individual within a facility. Facilities with high volumes of public contact and missions that are adversarial or controversial in nature may be subject to ramming attacks.

Facilities with limited acceleration areas or serpentine approaches reduce the potential approach speed of a ramming vehicle, and likely face a lower threat to this type of event.

Outlook

It is estimated that ramming attacks where the vehicle is the weapon will continue at an infrequent and unpredictable rate for the foreseeable future.

References

See Section 7.32

Vehicle Speed and Kinetic Energy Calculation

Maximum Vehicle Skidding Speed		
*Friction Coefficient:	1	Equation: $V_s=(fgr)^{1/2}$ Where: Vs = Skidding Speed f = Friction Coefficient g = Gravitational constant (32.2 ft/sec) ² r = Radius of curve
Radius of Curvature:	20	
Skidding Speed (mph)=	17.3	
<i>*The friction coefficient, a value between 0 and 1, depends on the size and type of tire, the material and condition of the drive path, and the traction afforded by the drive surface (e.g., dry or covered with oil, water, gravel or ice). A friction coefficient of 1.0 is the most conservative. A friction coefficient 0.6 is usually applicable for a dry surface paved road.</i>		

Maximum Attainable Vehicle Speed on a Straight Path		
*Acceleration Rate:	6	Equation: $V^2 = Vo^2 + 2as$ Where: V = Final vehicle speed Vo = Initial vehicle speed a = Acceleration s = Distance
**Initial Vehicle Speed (mph):	17.3	
Distance to the Target (feet):	100	
Vehicle Weight (lbs):	4700	
Maximum Attainable Speed (mph)=	29.3	
Kinetic Energy at Impact (1,000 ft/lb)=	134.73	
<i>*Acceleration rate of conventional vehicles is usually specified by the manufacturer. 11 ft/sec is typical for a high performance car and 6 ft/sec is typical for a 2-1/2 ton truck</i> <i>**The skidding speed is the initial vehicle speed in computing maximum attainable speed on a curved approach.</i>		

Maximum Attainable Vehicle Speed on a Sloped Path		
Acceleration Rate (a):	6	Correction Factor = $s'/s = 1/[1+(g/a)\sin\theta]$ Where: s' = Acceleration distance to attain final speed on a slope. s = Acceleration distance to attain final speed on a horizontal. g = Gravitational constant (32.2 ft/sec). a = Acceleration. q = Angle between the slope and the horizontal.
*Slope Angle (q):	2	
Distance to Target:	100	
Maximum Attainable Speed on Flat Path:	29.28	
Correction Factor (s'/s):	0.84	
Vehicle Weight:	4700	
Maximum Attainable Speed on a Slope:	34.8	
Kinetic Energy at Impact (1,000 ft/lb):	189.92	
*A negative angle reflects an upward slope and positive angle reflects a downward slope.		

Undesirable Event	7.31 Workplace Violence					
Definition	Violence perpetrated by an authorized occupant on an employee. The assailant can be another employee, authorized tenant, or an authorized visitor.					
Original Assessment	12-17-09	Revision	0	Date	N	
Classified Annex	No	Classification		Date		

Note: Workplace violence is often defined as any violence occurring in the workplace. The majority of the undesirable events addressed in the DBT document are forms of violence against employees, and thus all might be categorized "workplace violence." For the purposes of the DBT, "workplace violence" is limited to violence between co-workers. Other events address other violence which may be perpetrated against employees, including criminal and terrorist attacks.

Design-Basis Threat Scenario

An employee under duress from a job-related situation enters the facility and assaults co-workers using a handgun.

- OR -

Co-workers in the office get into a verbal confrontation resulting in one physically assaulting the other.

Baseline Threat

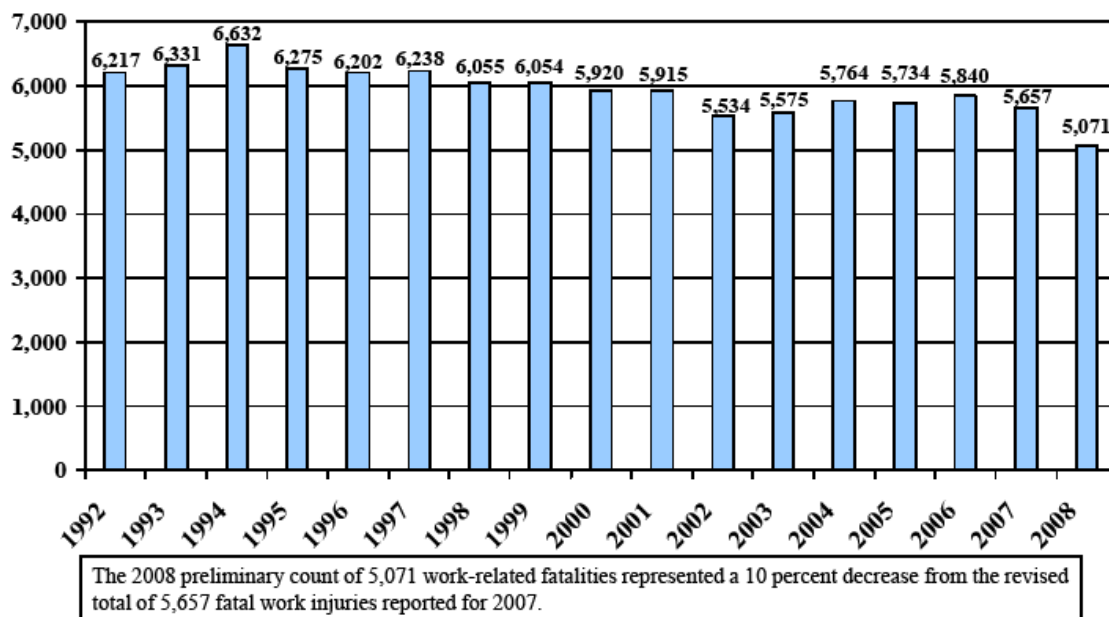
Based on the overall workplace violence statistics in the United States, to include various types of assault, abuse, and harassment, the baseline threat to Federal facilities from this event is assessed to be **HIGH**.

Analytical Basis

The Bureau of Labor Statistics cited an average of 1.7 million people were victims of violent crime each year while working or on duty from 1993 through 1999. Approximately 94 percent of the incidents reported were simple or aggravated assaults.

Between 1992 and 2008, an alarming rate of work-related fatalities occurred.

Number of fatal work injuries, 1992–2008*



*Data for 2008 are preliminary. Data for prior years are revised and final.
 NOTE: Data from 2001 exclude fatalities resulting from the September 11 terrorist attacks.
 SOURCE: U.S. Bureau of Labor Statistics, U.S. Department of Labor, 2009.

1

In 2007 alone, the Bureau of Labor Statistics reported 610 of the total fatalities for that year were homicides of which 491 involved shootings. Another fact reported was 22 percent of the homicides involved former employees and 43 percent involved current employees. Examples of these events include the following:

- On November 6, 2009, Jason Rodriguez entered the Legion Place office building in downtown Orlando, FL and made his way to the offices of Reynolds, Smith & Hills located on the 8th floor. Rodriguez, armed with a single handgun shot 6 employees, killing 1 and wounding 5 others. It was later reported Rodriguez had worked for the company and was fired in 2007. Rodriguez, who was overstressed with a myriad of problems and declining mental health, was reported to have blamed the company for “trouble with receiving his unemployment benefits” and “because they left him to rot”.
- On April 20, 2007, an employee who worked at the Communication and Tracking Development Laboratory, at the Lyndon B. Johnson Space Center (JSC) in Houston, Texas, shot and killed one person and took a hostage for over three hours before committing suicide. Police said the man was under review for poor job performance and he feared being dismissed.

7.31.2

- On December 26, 2000, an employee killed seven people at a Wakefield, Mass., Internet consulting company, Edgewater Technology. Authorities said the shooting may have stemmed from an Internal Revenue Service order to seize part of his wages to repay back taxes.
- On March 6, 1998, a former Connecticut Lottery accountant fatally shot four lottery executives, and then killed himself.
- On December 18, 1997, a fired employee killed four former co-workers at maintenance yard in Orange, CA.
- On August 20, 1986, a part-time letter carrier, facing possible dismissal after a troubled work history, walked into the Edmond, OK post office, where he worked and shot 14 people to death before killing himself. Though the most deadly, the Edmond tragedy was not the first episode of its kind in this period. In just the previous three years, four postal employees were killed by present or former coworkers in separate shootings in Johnston, South Carolina; Anniston, Alabama; and Atlanta, Georgia.
- Workplace violence, including assaults and suicides, accounted for 16 percent of all work-related fatalities in 2008. Homicides rank among the top four causes of workplace fatalities.

Target Attractiveness

Facilities with missions which involve high operational tempos or high-stress occupations may face a higher threat to this event. However, workplace violence can take place anywhere, and is often associated with life changing events personally or professionally. There is no profile of an employee who might become violent. With regards to work-related events in particular, termination, being passed over for a promotion or salary increase, interpersonal relationships, or disciplinary actions can initiate an acute stress environment for an employee.

Outlook

Workplace violence is now recognized as a specific category of violent crime that calls for distinct responses from employers, law enforcement, and the community. Statistics indicate a “rollercoaster” trend in the number of workplace incidents/fatalities covering more than the last 15 years. These statistics, coupled with the uncertainty and/or frequency of future incidents makes this type of event a viable threat within a facility.

Reference

See Section 7.32

7.32 Reference for Undesirable Events

- ⁱ www.cessna.com
- ⁱⁱ Excerpt: http://en.wikipedia.org/wiki/2010_Austin_plane_crash
- ⁱⁱⁱ HITRAC, 22 June 2006, Strategic Sector Assessment: U.S. Aviation
- ^{iv} Multiple web references
- ^v DHS/FBI JSA, Aviation Security Overview, 25 February 2005
- ^{vi} Homeland Security Threat Assessment: Evaluating Threats 2008-2013
- ^{vii} DHS Information Bulletin, Remotely Piloted Vehicle Threat, June 7, 2004
- ^{viii} DHS Information Bulletin, Remotely Piloted Vehicle Threat, June 7, 2004
- ^{ix} DHS Information Bulletin, Remotely Piloted Vehicle Threat, June 7, 2004
- ^x FBI/DHS IB Number, 141, Potential Terrorist Use of Helicopters, August 6, 2004
- ^{xi} Article posted by NEWS10/KXTV, (ABC affiliate), Sacramento, CA.
- ^{xii} TSA – INTEL Assessment, June 27, 2008
- ^{xiii} UNITED STATES ATTORNEY’S OFFICE, District of Oregon, 06/05/2007, Animal Liberation Front (ALF) and Earth Liberation Front (ELF) Members Sentenced in Oregon for Acts of Eco-Terrorism in Five Western States.
- ^{xiv} Tripwire Community Gateway, Terrorist Tactic: Arson, 2009.
- ^{xv} *Crime in the United States*, 2007, Federal Bureau of Investigation
- ^{xvi} *Crime in the United States*, 2007, Federal Bureau of Investigation
- ^{xvii} *Crime in the United States*, 2007, Federal Bureau of Investigation
- ^{xviii} *Crime in the United States*, 2007, Federal Bureau of Investigation
- ^{xix} Excerpt: <http://www.cnn.com/2010/CRIME/01/04/las.vegas.shooting/index.html>
- ^{xx} Wikipedia

^{xxi} Excerpt: http://www.phillyburbs.com/news/news_details/article/2504/2010/march/04/2-pentagon-police-officers-shot-1.html

^{xxii} Excerpt: <http://www.csmonitor.com/USA/2010/0219/IRS-a-frequent-target-of-antigovernment-violence>

^{xxiii} Potential Terrorist Attack Methods

^{xxiv} Potential Terrorist Attack Methods

^{xxv} GAO-04-133T, Testimony before the Committee on Homeland Security, Counterfeit Identification Raises Homeland Security Concerns, October 1, 2003

^{xxvi} Dennis Blair, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, U.S. Senate*, February 12, 2009.

^{xxvii} Domestic Terrorists' Intent and Capability to Use Chemical, Biological, Radiological, and Nuclear Weapons, 14 October 2008

^{xxviii} "Iraq gas attack makes hundreds ill". CNN, 3/18/2007

^{xxix} 'Chlorine bomb' hits Iraq village". BBC News. 5/17/2007

^{xxx} Excerpt: Information Bulletin (REVISED) Title: Potential Terrorist Exploitation of Heating, Ventilation, and Air Conditioning (HVAC) Systems Date: September 27, 2004

^{xxxi} Dennis Blair, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, U.S. Senate*, February 12, 2009.

^{xxxii} Domestic Terrorists' Intent and Capability to Use Chemical, Biological, Radiological, and Nuclear Weapons, 14 October 2008

^{xxxiii} Domestic Terrorists' Intent and Capability to Use Chemical, Biological, Radiological, and Nuclear Weapons, 14 October 2008

^{xxxiv} Dennis Blair, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, U.S. Senate*, February 12, 2009.

^{xxxv} Domestic Terrorists' Intent and Capability to Use Chemical, Biological, Radiological, and Nuclear Weapons, 14 October 2008

(U) Homeland Security Threat Assessment: Evaluating Threats 2008-2013, DHS Special Compilation of Topical Information on Ricin, James Martin Center for Nonproliferation Studies, February 29, 2008

(U) Domestic Terrorists' Intent and Capability to Use Chemical, Biological, Radiological, and Nuclear Weapons, Joint Special Assessment, DHS and FBI

^{xxxvi} Dennis Blair, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, U.S. Senate, February 12, 2009.

^{xxxvii} Domestic Terrorists' Intent and Capability to Use Chemical, Biological, Radiological, and Nuclear Weapons, 14 October 2008

^{xxxviii} USAF Research Laboratory Food and Water Vulnerability Database, November 1999

^{xxxix} JHSA - Water Systems at Risk to Deliberate Contamination, 6 March 2008

^{xl} FBI Intelligence Assessment - Threat of Terrorists Contaminating or Disrupting U.S. Drinking Water at Treatment and Storage Facilities (U), March 20, 2006

^{xli} FBI Intelligence Assessment - Threat of Terrorists Contaminating or Disrupting U.S. Drinking Water at Treatment and Storage Facilities (U), March 20, 2006

^{xlii} FBI Intelligence Assessment - Threat of Terrorists Contaminating or Disrupting U.S. Drinking Water at Treatment and Storage Facilities (U), March 20, 2006

^{xliii} Potential Bioterrorism Threats to U.S. Public Water Supplies (U), Science and Technology Expert Partnership, November 15, 2002

^{xliv} Potential Bioterrorism Threats to U.S. Public Water Supplies (U), Science and Technology Expert Partnership, November 15, 2002

^{xliv} Potential Bioterrorism Threats to U.S. Public Water Supplies (U), Science and Technology Expert Partnership, November 15, 2002

Water and terrorism, Peter H. Gleick, Pacific Institute, August 14, 1996

Potential Bioterrorism Threats to U.S. Public Water Supplies (U), Science and Technology

Expert Partnership, November 15, 2002

Mujahedeen Poisons Handbook

FBI Intelligence Assessment - Threat of Terrorists Contaminating or Disrupting U.S. Drinking Water at Treatment and Storage Facilities (U), March 20, 2006

^{xlvi} The Star, Kansas City, MO

^{xlvi} CNN

^{xlvi} DHS Tripwire

^{xlvi} New York Times

ⁱ Source: Washington Post

^{li} DHS IA, Recently Discovered Al-Qa'ida Training Material Targets Public Buildings, 6 October 2008

^{lii} FBI Intelligence Assessment - Threat of Terrorists Contaminating or Disrupting U.S. Drinking Water at Treatment and Storage Facilities (U), March 20, 2006

^{lii} Excerpt: United States Department of Homeland Security, Tripwire, Community Gateway, *Structural Sabotage*

^{liv} Criminal Complaint, United States of America vs. Michael C. Finton (a.k.a. "Talib Islam")

^{lv} Behavior and Characteristics of bomb related offenders, National Center for the Analysis of Violent Crime

Overpressure curve calculated using A.T.-Blast version 2.2

^{lvi} Arrest Warrant, United States of America vs. Hosam Maher Husein Smadi

^{lvii} Criminal Complaint, United States of America vs. Michael C. Finton (a.k.a. "Talib Islam")

^{lviii} GAO Report GAO-09-801T

Overpressure curve calculated using A.T.-Blast version 2.2

^{lix} Excerpt: <http://www.cbsnews.com/stories/2005/06/20/national/main703102.shtml>

^{lx} Excerpt: TERRORISM PREVENTIONS
http://www.fbi.gov/publications/terror/terror2000_2001.pdf

-
- ^{lxi} <http://www.splcenter.org/get-informed/publications/terror-from-the-right>
- ^{lxii} JHSA- Possible Suicide Bomber Planning Behavior and Point-of-Attack Indicators, 27 September 2006
- ^{lxiii} Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005
- ^{lxiv} JHSA, Terrorist Tradecraft Involving Suicide Bombers, 31 August 2006
- Overpressure curve calculated using A.T.-Blast version 2.2
- ^{lxv} Banking and Financial Services Sector Threat Assessment, April 19, 2007)
- ^{lxvi} JIB - Al-Qa'ida Surveillance Tactics Similar to Those in Recovered Training Manual (U), September 15, 2004
- ^{lxvii} - Use of Technology in Terrorist Surveillance Techniques, 19 December 2005
- ^{lxviii} JIB - Use of Technology in Terrorist Surveillance Techniques, 19 December 2005
- ^{lxix} JHSA- Possible Suicide Bomber Planning Behavior and Point-of-Attack Indicators, 27 September 2006
- ^{lxx} Quoted from: The United States Department of Homeland Security and the Federal Bureau of Investigation, Joint Information Bulletin, *Recent Terrorist Plots Highlight Insider Threat*, August 7, 2007
- ^{lxxi} Quoted from: The United States Department of Homeland Security and the Federal Bureau of Investigation, Joint Information Bulletin, *Terrorist Attack Planning and "Dry Run" Tactic Indicators*, August 30, 2007
- ^{lxxii} JHSA - Webcams: A Potential Terrorist Planning Tool, 10 January 2007
- ^{lxxiii} Excerpt from: 3:47 a.m. EDT, Sun June 14, 2009 (*CNN*) article
- ^{lxxiv} Outline of the Fundamentals in the Art of Kidnapping Americans, TRIPwire
- ^{lxxv} Second National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children (NISMAART-2)
- ^{lxxvi} Office of Juvenile Justice and Delinquency Programs, Juvenile Justice Bulletin, Kidnapping of Juveniles: Patterns from NIBRS, June 2000.

^{lxxvii} Second National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children (NISMART–2)

^{lxxviii} Second National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children (NISMART–2)

^{lxxix} Second National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children (NISMART–2)

^{lxxx} Excerpt from: United States Department of Homeland Security, Tripwire, Community Gateway, *Terrorist Tactic: Kidnapping/Hostage Taking*

^{lxxxi} FBI Intelligence Assessment – Chemical Sector: Potential Target for Attack, Theft, and Diversion of Materials, July 27, 2009

^{lxxxii} FBI Intelligence Assessment – Chemical Sector: Potential Target for Attack, Theft, and Diversion of Materials, July 27, 2009

^{lxxxiii} Intelligence Assessment – Chemical Sector: Potential Target for Attack, Theft, and Diversion of Materials, July 27, 2009

^{lxxxiv} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{lxxxv} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{lxxxvi} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{lxxxvii} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{lxxxviii} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{lxxxix} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{xc} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{xci} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{xcii} *Crime in the United States*, 2007, Federal Bureau of Investigation

DOS SD-STD-01.01, Certification Standard for Forced Entry and Ballistic Resistance of Structural Systems provides three different forcible entry resistance certification tests: 5, 15, and 60 minutes. The 5 minute test is performed with two adversaries, while the 15 and 60 minute tests are performed using teams of 6 adversaries. The type and amount of forcible entry tools increases for each test.

UFGS- 08 34 01 Forced Entry Resistant Components guide spec.

ASTM F 588 - windows

ASTM F 842 – sliding doors

ASTM F 476 – swinging doors

^{xciii} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{xciv} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{xcv} Excerpt from: *Data center robbery leads to new thinking on security*, Patrick Thibodeau, Computerworld, 7 January 2008

^{xcvi} *Crime in the United States*, 2007, Federal Bureau of Investigation

DOS SD-STD-01.01, Certification Standard for Forced Entry and Ballistic Resistance of Structural Systems provides three different forcible entry resistance certification tests: 5, 15, and 60 minutes. The 5 minute test is performed with two adversaries, while the 15 and 60 minute tests are performed using teams of 6 adversaries. The type and amount of forcible entry tools increases for each test.

UFGS- 08 34 01 Forced Entry Resistant Components guide spec.

ASTM F 588 - windows

ASTM F 842 – sliding doors

ASTM F 476 – swinging doors

^{xcvii} *Crime in the United States*, 2007, Federal Bureau of Investigation

^{xcviii} *Crime in the United States*, 2007, Federal Bureau of Investigation