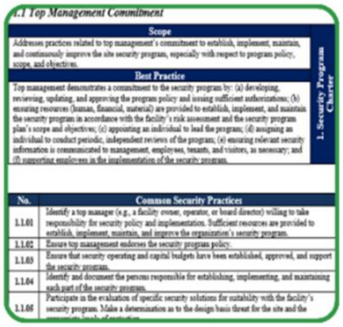
Field Guide: Conducting BPATS Based Assessments of Commercial Facilities

(BPATS - Best Practices for Anti-Terrorism Security)

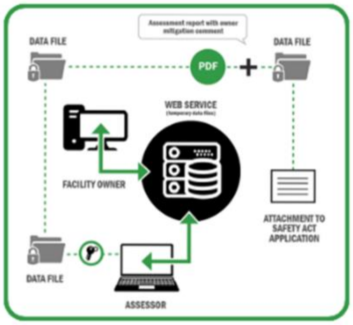


.1 Top Management Commitment

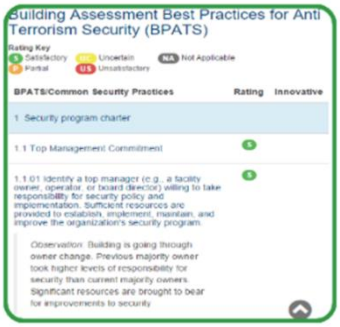
Scope	1. Security Program Charter
Addresses practices related to top management's commitment to establish, implement, maintain, and continuously improve the site security program, especially with respect to program policy, scope, and objectives.	
Best Practice	
Top management demonstrates a commitment to the security program by: (a) developing, reviewing, updating, and approving the program policy and issuing sufficient authorizations; (b) ensuring resources (human, financial, material) are provided to establish, implement, and maintain the security program in accordance with the facility's risk assessment and the security program plan's scope and objectives; (c) appointing an individual to lead the program; (d) assigning an individual to conduct periodic, independent reviews of the program; (e) ensuring relevant security information is communicated to management, employees, tenants, and visitors, as necessary; and (f) supporting employees in the implementation of the security program.	

No.	Common Security Practices
1.1.01	Identify a top manager (e.g., a facility owner, operator, or board director) willing to take responsibility for security policy and implementation. Sufficient resources are provided to establish, implement, maintain, and improve the organization's security program.
1.1.02	Ensure top management endorses the security program policy.
1.1.03	Ensure that security operating and capital budgets have been established, approved, and support the security program.
1.1.04	Identify and document the persons responsible for establishing, implementing, and maintaining each part of the security program.
1.1.05	Participate in the evaluation of specific security solutions for suitability with the facility's security program. Make a determination as to the design basis threat for the site and the appropriate levels of protection.

BPATS 1.1 Top Management Commitment



BPATS Assessment Tool Flowchart



Building Assessment Best Practices for Anti Terrorism Security (BPATS)

Rating Key

S Satisfactory UC Uncertain NA Not Applicable

P Partial US Unsatisfactory

BPATS/Common Security Practices	Rating	Innovative
1 Security program charter		
1.1 Top Management Commitment	S	
1.1.01 Identify a top manager (e.g., a facility owner, operator, or board director) willing to take responsibility for security policy and implementation. Sufficient resources are provided to establish, implement, maintain, and improve the organization's security program.	S	

> *Observation:* Building is going through owner change. Previous majority owner took higher levels of responsibility for security than current majority owners. Significant resources are brought to bear for improvements to security

BPATS Assessment Tool Input Screen

August 2018

The BPATS Assessment Tool (the "Tool") was developed by the National Institute of Building Sciences (Institute) under contract to the United States Department of Homeland Security (DHS), Science and Technology Directorate, Office of the SAFETY Act Implementation (OSAI). Both the Institute and the United States Government own and hold property rights and interests in and to the Tool and reserve all such rights therein. You are hereby permitted to use the Tool for its intended purpose of assessing the security features, practices and procedures of your commercial facility. Use of the Tool for purposes for which it is not intended is hereby prohibited. You may not reproduce and publish or otherwise distribute or display the Tool to others for commercial or other unauthorized purposes. You may not modify the Tool or create derivative works based on the Tool without express written approval of both the Institute and the DHS OSAI.

DISCLAIMER: NEITHER THE INSTITUTE, THE DHS, NOR THE UNITED STATES GOVERNMENT WARRANTS OR GUARANTEES THAT USE OF THE BPATS ASSESSMENT TOOL WILL PROTECT USER, USER'S FACILITY, OR PERSONS OCCUPYING USER'S FACILITY FROM HARM, INJURY, LOSS OR DAMAGES CAUSED BY TERRORIST OR OTHER CRIMINAL ACT DIRECTED AGAINST THE FACILITY OR ITS OCCUPANTS. NEITHER THE INSTITUTE NOR THE UNITED STATES GOVERNMENT, OR ANY AGENCY OR DEPARTMENT THEREOF, ASSUMES ANY LIABILITY WHATSOEVER FOR INJURY, LOSS OR DAMAGES INCURRED BY A FACILITY OR ANY PERSON(S) OCCUPYING A FACILITY BASED UPON OR ALLEGED TO BE BASED UPON USE OF THIS BPATS ASSESSMENT TOOL FOR COMMERCIAL FACILITIES.

Acknowledgments

The Office of SAFETY Act Implementation, Science and Technology Directorate, Department of Homeland Security (DHS) acknowledges the assistance of the National Institute of Building Sciences in the development of this Field Guide and revising and expanding the original Best Practices for Anti-Terrorism Security and the process identified in the "The Manual for Assessors for Anti-Terrorism Facility Security Systems Metropolitan Commercial Office Buildings, DHS, Pre-Decisional 2015." on which this Field Guide is based.

The Office of SAFETY Act Implementation also acknowledges Homeland Security Studies and Analysis Institute (HSSAI) for compiling the original Best Practices for Anti-Terrorism Security and developing the original manual. HSSAI is a Federally Funded Research and Development Center established for the DHS.

Project Officer

Bruce Davidson, Department of Homeland Security (DHS), Science and Technology Directorate, Office of the SAFETY Act Implementation (OSAI)

Project Managers

Leya Posey, Department of Homeland Security (DHS), Science and Technology Directorate, Office of the SAFETY Act Implementation (OSAI)

Roger Grant, National Institute of Building Sciences

Author

Terrence Ryan, TRyan AT FP, LLC

Software Developer

Bob Payne, National Institute of Building Sciences

Contributors

Earle Kennett, National Institute of Building Sciences

Table of Contents

1. Introduction

The Department of Homeland Security (DHS) has national leadership responsibilities for managing risks involving critical infrastructure, key resources, and events. DHS has identified commercial facilities as key assets in the critical infrastructure/ key resource sector and encourages the widespread deployment of effective anti-terrorism technologies, services and capabilities. Building security programs are a technology that may receive Designation under the SAFETY Act.

To help commercial building owners and managers, the Science and Technology Directorate, Office of SAFETY Act Implementation identified a set of best operational security practices for metropolitan commercial office buildings, referred to as Best Practices for Anti-Terrorism Security or BPATS. This list is available to owners and assessors in this Field Guide.

There was also a need for an assessment methodology that could be used to record and compare a facility's practices to the BPATS. This Field Guide and the associated online tool meets that need by providing a recommended process that can be used to improve the content and persuasiveness of assessments.

2. Overview

The guide starts with the key concepts of a BPATS based assessment and then provides information on the three-phase assessment process: The Documentation Review phase, the Site Visit phase, and the Report Development phase. The guide finishes with a review of Owner / Operator post assessment actions. Appendix A of the Guide contains the BPATS list. Seven practice categories are used to organize the 24 BPATS. There are 411 Common Security Practices in the 24 BPATS and the determination of the extent to which the Building Security program incorporates each of these BPATS' is a key part of the assessment.

3. Key Assessment Concepts

As we go through the process, there are several key concepts to remember.

- First, this is an assessment process using best practices for anti-terrorism security, or BPATS, not for all hazards. Vulnerabilities to other threats, such as earthquakes, floods or other natural hazards, may not be discovered through this process.
- The assessment is not a pass / fail process; it is the description of a snapshot in time of a building's security program. Few, if any, security programs will meet all best practices.
- Assessments should identify notable strengths as well as areas that may need further development.
- When performing an assessment think beyond a "conformity assessment" and ask, "is the system effective in facilitating the defense against acts of terrorism?" Use the list of BPATS to organize the report, but not to limit the findings and assessment.
- Whatever the findings are to the best practice comparison, remember they need to be evidence based. For example, they should state written policy evidence, plus records or incident report evidence to support the finding.

- Assessment reports must include a clear statement of scope of the assessment and define any assumptions and limitations. For example: the scope could be the security program for just a project's high-rise, or the high-rise and a plaza, or the high-rise, plaza and the parking garage.
- The BPATS-based assessment covers physical methods of attack to personnel and tangible property, with an emphasis on terrorism. Methods of attack may be split into two broad categories: physical threats to personnel and tangible property, and threats of electronic or computer-based attacks on the information systems. The BPATS based assessment described in this guide only covers the physical methods of attack, not computer-based attacks on the information systems. For cyber threats, there are other cyber assessment tools like the CSET (Cyber Security Evaluation Tool). Please note however, there is a section on "Information Security" included in the BPATS, which addresses the physical protections of IT systems.

4. Assessment Scope

Before starting an assessment, confirm the assessment's scope. An assessment scope statement is an essential element of any project. It is a tool used to describe the major deliverables of a project including the key milestones, high level requirements, assumptions, and constraints. It also defines the boundaries of a given project and clarifies what deliverables are in and out of scope.

Note: If the Assessment report is included as part of a SAFETY Act Application, the assessment scope statement will be compared to the SAFETY Act Application Technology Description.

5. Assessment Process

The BPATS based assessment process consists of three steps:

- Step 1: Review documentation to determine if facility management has properly established, implemented, and maintained an anti-terrorism security program
- Step 2: Visit the site to visually establish that the security system functions and infrastructure are in place and operational
- Step 3: Complete an assessment report that documents findings. These findings should be detailed and should be based in evidence found in steps 1 and 2.

More than one assessor may conduct the assessment. For example, a Physical Security Subject Matter Expert (SME) and a Building Systems SME may form a team and divide the work appropriately.

Before any work is done, assessors should expect to establish a non-disclosure agreement (NDA) with the owner / manager. The NDA may help with information exchange and information in the NDA is listed as a part of the final report.

5.1. Documentation Review

Documentation review is the first step in the assessment process. Documentation provides evidence about how a building's security program has been established, implemented and maintained. This review may be done prior to the site visit if you are allowed access to documents, or if documents are not released, it may be done during the first part of the on-site assessment. Items to review include management documents, such as staffing, organization and budgeting guidance; plans such as the emergency action plan, the continuity of operations plan and the tenant handbook; reports and studies such as an engineering analysis on blast; as well as facility and security force policies and procedures.

First, conduct a brief review to make sure the site has enough information to conduct a security review with respect to the BPATS. As needed, request missing information from the facility. If there is not enough documentation, you should delay the assessment until the necessary documentation is available.

Next, determine how each document or record provides or does not provide adequate evidence of a Best Practice - think of this as a two or three-point verification with a clear record of recent actions or events. For example, there should be a security plan plus a record of quarterly meetings reviewing the program; a written security procedure plus an after-action report from the latest incident response; and a security system layout and design concept, in addition to records of quarterly tests, repairs and maintenance.

Finally, cross check the documents to ensure the policies and procedures correlate. For example, the same list of hazards in the Continuity of Operations plan should also be addressed in the Tenant Handbook and in the Security Force Procedures.

5.1.1. Document Review List

The document list is a mixture of items: some are evidence of a best practice and some facilitate and support the assessment. For example:

- Floor plans facilitate site tours and understanding the buildings layout and design
- Exercise After Action Reports are evidence how the building's security program is being testing and improved

Recommended documentation to review is listed in the table below. Next to each document is a reference to the corresponding BPATS or a note that the document is a facilitating and supporting item. In addition to the types of documentation listed, you may consider any other types of documents and records relevant to the assessment scope. (*See TABLE 1: DOCUMENTATION REVIEW LIST)*

Document	BPATS Reference
Building Plans and Elevations	(facilitating and supporting item)
Building Interior Diagrams and Layouts	(facilitating and supporting item)
Incident Response Plans	2.3 Incident Preparedness, 2.4 Incident Response and Recovery
Security Policies (Building Occupants)	1.1 Top Management Commitment, 1.2 Policy, 2.2 Risk Awareness, 3.3 Information Security
Security Staff Procedures (i.e. Post Orders)	2.1 Risk Assessment, 2.3 Incident Preparedness, 2.4 Incident Response and Recovery, 2.5 Continuity of Operations, 3.1 People Surety, 3.2 Identification and Verification, 3.3 Information Security, 4.2 Systems, 5.1 Policies and Procedures, 6.3 Controlled and Restricted Areas

Document	BPATS Reference
Continuity of Operations Planning	2.1 Risk Assessment, 2.3 Incident Preparedness, 2.5 Continuity of Operations
Training Records of the Security Staff	3.1 People Surety
Incident Reports	2.1 Risk Assessment, 7.2 Evaluation
Life Safety System Inspection Reports including Open Violation Progress Reports	(facilitating and supporting item)
Risk Assessments and Threat Assessments	1.2 Policy, 1.3 Scope and Objectives, 2.1 Risk Assessment, 2.3 Incident Preparedness, 3.3 Information Security, 5.1 Policies and Procedures, 7.2 Evaluation
Building Construction Specifications	(facilitating and supporting item)
Plans depicting the location of fire, camera and security systems	(facilitating and supporting item)
Security Program Audit Reports	7.2 Evaluation
Security tests or table top exercise records	2.4 Incident Response and Recovery, 3.3 Information Security, 7.1 Exercising and Testing, 7.2 Evaluation
Diagram listing the location of technology assets controlled by building management such as electronic mail or web servers, data centers, networking nodes, controlled interface equipment and communications equipment	(facilitating and supporting item)
Engineering Analysis on Blast Protection	6.1 Physical Structure, 6.3 Controlled and Restricted Areas
Design Basis Threat (DBT) for Terrorism (i.e. External/Internal Blast, External/ Internal CBRN Release, External/Internal Armed Attack and Physical Attack or Tampering of IT Systems)	1.1 Top Management Commitment, 1.2 Policy, 2.1 Risk Assessment
Business Impact Assessment	2.1 Risk Assessment, 2.3 Incident Preparedness, 2.5 Continuity of Operations, 7.2 Evaluation

TABLE 1: DOCUMENTATION REVIEW LIST

5.1.2. Document Rating Scale

In the assessment report, rate the documents that provide or do not provide evidence of a best practice and comment on items missing or incomplete. A simple scale used in the BPATS Assessment Tool is listed here:

AA	Available, meets needs and attached
AR	Available, meets needs but restricted and not attached
AI	Available but Incomplete
NP	Not Present

Assessors should rely on their training and experience to make this Rating determination. When numerous records are available, assessors should review a sample of those records. For example, if security officers are required to fill out a checklist for inspections, assessors should review a reasonable number of the checklists.

As part of this documentation review, you should determine if the evidence contained in the documentation comes from appropriate sources. That is, are there signed and dated internal records related to the security system and after-action reports from third-party organizations?

5.2.Site Visit

The second step in the assessment process is a site visit. The purpose of the site visit is to record how well the Building Security Program (within the limits of the scope of the assessment) compares to each of the 411 Common Security Practices and the 24 BPATS or other applicable security practices. You can determine this by observing the site layout and design, interviewing the facility staff and/or contractors, witnessing operations, and reviewing additional documentation found during the tour.

One underlying question is: “Do the plans and procedures match the current operations?” Pay close attention to issues or areas of uncertainty discovered during the documentation review.

5.2.1. Site Visit Plan

Before the site visit, the you should develop a site visit plan. The site visit plan serves as the road map for the visit and sets expectations for both parties. The OSAI recommends including the Site Visit Plan in facility assessment reports as evidence of an organized assessment.

At a minimum, the Site Visit Plan should include the following:

- Tour all aspects of the facility and its security systems;
- Interview facility staff and/or contractors;
- Compare policy to current operations; and
- Identify facility assets, threats, and vulnerabilities.

The site visit plan serves as the road map for the site visit and sets expectations for both parties.

A key step in this process is to coordinate with the facility before the visit. Pre-visit coordination (both by e-mail and teleconference) can be used to set objectives based on the facility’s characteristics, notify the site of the expected duration of the visit, and identify the resources needed to conduct the assessment. Thorough preparation will optimize time spent at the site.

5.2.2. Assets, Functions, Infrastructure

One way to gain different perspectives of the facility during the site visit is to look at the facility’s assets, functions, and infrastructure separately. This simplifies an understanding of how the facility may be affected by a terrorist act. The below table lists areas to consider in each category. (*See TABLE 2: ASSETS, FUNCTIONS, INFRASTRUCTURE*)

Assets	Functions	Infrastructure
•Occupants •Materials •Replacement Value •Local / Regional Impact	•Building Management •Security Operations and Management •Security Forces •Planning and Exercises •Engineering Operations and Maintenance •Business Continuity •Vendors	•Site •Architecture •Building Envelope •Structural Components and Systems •Mechanical / Electrical / Utilities •IT and Communication •Fire Alarm Systems •Security Systems

Table 2: Assets, Functions, Infrastructure

Assets include the occupants and materials. Consider the replacement value of those assets, and also consider the local/regional impact from the loss of those assets. You should consider not only the occupants during a normal day, but also at peak levels, when employees, visitors, and vendors are on site. This number should not include brief influxes in population as an occasional conference (or similar event), unless the facility is intended for use in such a manner (like a conference center) and the population is part of normal business. Remember to consider high value or bulk materials present and their replacement value.

Functions include Building Management, Security Operations and Management, Facility Engineering and others. Consider which functions have to operate 24/7 and which may be delayed following an event.

Finally, you need to look at the site's infrastructure. This is a challenging task, since the infrastructure is a complex interrelated system. Look at each component separately, but also consider how each infrastructure component functions in related systems and in the larger system as a whole. For example, mechanical/electrical/utilities will be closely linked with everything from IT and Communication, to fire alarms, and security systems.

Get in the habit of looking at different systems multiple times from different perspectives as you conduct your visit.

5.2.3. Tour Checklist

Before the site visit, your assessment team should develop a Tour Checklist. Establishing a checklist is a good method for ensuring you accomplish your site visit goals.

First, you need to ensure that the tour will meet the assessment objectives and scope, as well as the Best Practice requirements. For example, there are practices concerning parking. If the parking area is in the scope of the assessment, then it needs to be part of the tour. If the building uses a parking facility in a separate building across the street and it is not in the scope of the assessment, then the parking practices are non-applicable, and the parking facility does not need to be on the site tour checklist.

Second, you need to observe the building's security program in action. Ways to do this are to watch security staff perform their duties, request to witness common security activities, such as visitor processing, and observe a normally scheduled test of security equipment, systems, or capability.

Third, you should confirm that documented plans, policies, and procedures reflect actual practice.

Finally, the tour checklist should include looking at adjacent facilities. These nearby facilities may increase target attractiveness, or you may be at risk from "collateral damage" from an attack on an adjacent site.

The following list is a starting point for planning your visit, and may be adapted as needed:

- Adjacent Facilities
- Air Intakes
- Building Perimeter
- Data / Telephone Systems: Centers, Demarcation Point, Distribution Systems and Closets
- Emergency Generator/ fuel
- Emergency Operations Center
- Engineering Control Center
- Exterior Entrances
- Fire Control Center
- Fuel Storage
- Lobbies
- Loading Dock
- Mailroom
- Major Mechanical, Electrical and Plumbing Systems
- Parking Areas
- Roof Access
- Security Control Center
- Warehouse
- Water Supply

5.2.4. Threats

Building security programs are affected by changing threats. The topic of "Threats" is addressed in eight of the Common Security Practices and an understanding of unique threats to the facility is an important part of an assessment. As part of the site visit, ask the building owner / representative to review their threat assessment. If they have a Threat Assessment, analyze it with them. If appropriate, include it in your assessment.

If the owner does not have a threat assessment, conduct an analysis with them and determine the threats you will consider in your assessment. A good tactic for doing this is to first list all possible threats and then tailor that list for the facility.

For example, first consider all possible threats to the facility, such as the below extract from: *The Risk Management Process: An Interagency Security Committee Standard Appendix F: Forms & Templates,* *Aug 2013 (Document marked: Distribution of this document to Federal, State, local agencies, and private individuals or enterprises is authorized.)*

- Aircraft as a Weapon
- Arson
- Assault
- Ballistic Attack - Active Shooter
- Ballistic Attack - Small Arms
- Ballistic Attack - Standoff Weapons
- Breach of Access Control Point - Covert
- Breach of Access Control Point - Overt
- CBR Release - External
- CBR Release - Internal
- CBR Release - Mailed or Delivery
- CBR Release - Water Supply
- Civil Disturbance
- Disruption of Facility or Security Systems
- Explosive Device - Man-Portable External
- Explosive Device - Man-Portable Internal
- Explosive Device – Suicide / Homicide
- Explosive Device - Vehicle Borne IED
- Explosive Device - Mail or Delivery
- Hostile Surveillance
- Insider Threat
- Kidnapping
- Release of Onsite HAZMAT
- Robbery
- Theft
- Unauthorized Entry - Forced
- Unauthorized Entry - Surreptitious
- Vandalism
- Vehicle Ramming
- Workplace Violence
- Coordinated or Sequential Attack

Second: tailor the same list based on your information of the terrorist threat and add any additional unique threats to the facility. As a hypothetical example, you might have started with 31 possible threats and then tailored the list down to the 27 that fit your facility as illustrated below.

- ~~Aircraft as a Weapon~~
- Arson
- Assault
- Ballistic Attack - Active Shooter
- Ballistic Attack - Small Arms
- Ballistic Attack - Standoff Weapons
- Breach of Access Control Point - Covert
- Breach of Access Control Point - Overt
- CBR Release - External
- CBR Release - Internal
- CBR Release - Mailed or Delivery
- CBR Release - Water Supply
- ~~Civil Disturbance~~
- Disruption of Facility or Security Systems
- Explosive Device - Man-Portable External
- Explosive Device - Man-Portable Internal
- Explosive Device – Suicide / Homicide
- Explosive Device - Vehicle Borne IED
- Explosive Device - Mail or Delivery
- Hostile Surveillance
- Insider threat
- Kidnapping / Hostage Taking
- Release of Onsite HAZMAT
- Robbery
- ~~Theft~~
- Unauthorized Entry - Forced
- Unauthorized Entry - Surreptitious
- ~~Vandalism~~
- Vehicle Ramming
- Workplace Violence
- Coordinated or Sequential Attack

5.2.5. Comparison analysis to Best Practices for Anti-Terrorism Security (BPATS)

During the site visit, conduct a comparison analysis of the current security practices to the BPATS and their related Common Security Practices. See *BEST PRACTICES FOR ANTI-TERRORISM SECURITY (BPATS) LIST FOR COMMERCIAL OFFICE BUILDINGS,* DHS Office of SAFETY Act Implementation, for the complete BPATS listing. For conducting the comparison, it is recommended to use the automated BPATS worksheets in the online tool: *BPATS Assessment Tool for Commercial Facilities.* The tool may be found at: https://bpatsassessmenttool.nibs.org

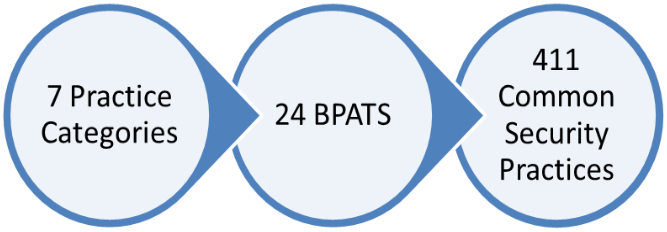
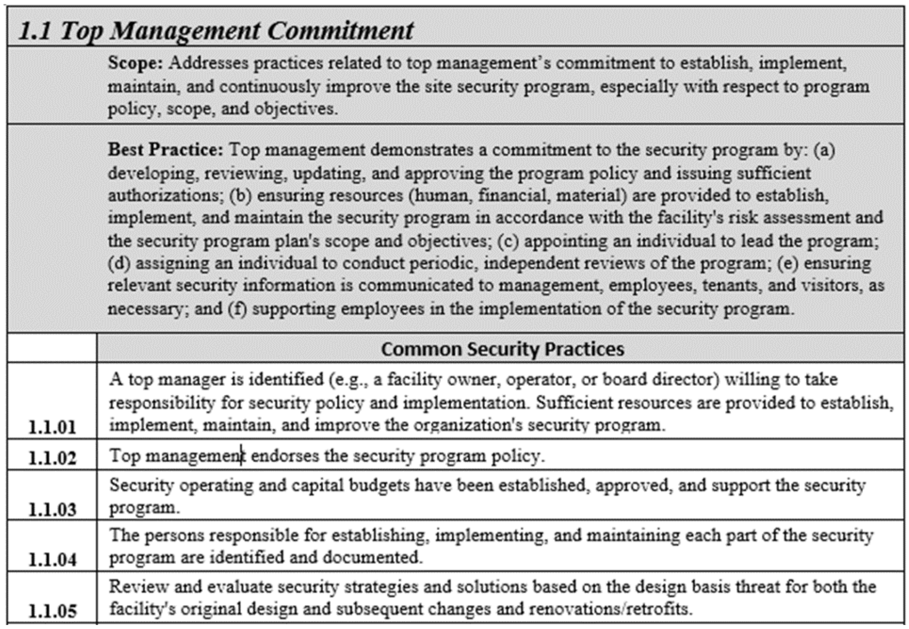


DIAGRAM 1: BPATS TAXONOMY

To organize the comparison, the following taxonomy has been established (SEE DIAGRAM 1: BPATS TAXONOMY):

- At the highest level there are 7 Practice Categories used to organize the 24 Best Practices for Anti-Terrorism Security or BPATS. Each Practice Category contains two to five related BPATS, for a total of 24 BPATS.
- Under each individual BPATS, there are three to 60 associated Common Security Practices for a total of 411 Common Security Practices.

Each BPATS includes: A Scope Statement; a Best Practice Statement, which identifies the outcome specified by the best practice (in other words, the requirements); and a list of Common Security Practices. (*See Diagram 2, Extract of BPATS 1.1 Top Management Commitment*)



1.1 Top Management Commitment	
	Scope: Addresses practices related to top management's commitment to establish, implement, maintain, and continuously improve the site security program, especially with respect to program policy, scope, and objectives.
	Best Practice: Top management demonstrates a commitment to the security program by: (a) developing, reviewing, updating, and approving the program policy and issuing sufficient authorizations; (b) ensuring resources (human, financial, material) are provided to establish, implement, and maintain the security program in accordance with the facility's risk assessment and the security program plan's scope and objectives; (c) appointing an individual to lead the program; (d) assigning an individual to conduct periodic, independent reviews of the program; (e) ensuring relevant security information is communicated to management, employees, tenants, and visitors, as necessary; and (f) supporting employees in the implementation of the security program.
	Common Security Practices
1.1.01	A top manager is identified (e.g., a facility owner, operator, or board director) willing to take responsibility for security policy and implementation. Sufficient resources are provided to establish, implement, maintain, and improve the organization's security program.
1.1.02	Top management endorses the security program policy.
1.1.03	Security operating and capital budgets have been established, approved, and support the security program.
1.1.04	The persons responsible for establishing, implementing, and maintaining each part of the security program are identified and documented.
1.1.05	Review and evaluate security strategies and solutions based on the design basis threat for both the facility's original design and subsequent changes and renovations/retrofits.

DIAGRAM 2: EXTRACT OF BPATS 1.1: TOP MANAGEMENT COMMITTMENT

The Common Security Practices are suggested anti-terrorism actions, procedures, methods, or systems used to execute the outcome specified by the best practice. BPATS are not compliance items, but goal-oriented statements of anti-terrorism security objectives. Conducting a comparison is a way to collect information, and this requires that you ask more than just "Yes" or "No" questions. Analyzing how the buildings security program compares with a Best Practice should result in specific and detailed findings.

As such, this comparison process requires an experienced assessor with prior knowledge of security engineering principles. Assessor's need to have an understanding of concepts, such as "progressive collapse", "blast effects", and "biological and chemical properties" to be effective.

Other concepts include, "layered defense" and "detect, assess, delay, and respond". You will need to use this knowledge as a lens for viewing the security practices discussed in the BPATS.

The BPATS list is not finite: i.e. it does not cover local building code, life safety, or HAZMAT requirements. However, any open violations of these requirements should be considered. Assessors may also consider security practices not listed.

5.2.6. Best Practices for Anti-Terrorism Security (BPATS) Ratings

During and/or following the site visit, complete an assessment worksheet for each of the BPATS and their related Common Security Practices. The assessment worksheet has a place to record a rating for each BPATS and Common Security Practice and also your rationale for the rating. There is no set number of Common Security Practices necessary to achieve a "Satisfactory" BPATS rating. You will need to rely on your expertise and experience to rate the comparison of the practice.

The recommended rating scale is: Satisfactory, Partial, Unsatisfactory and Uncertain. In your assessment report, any Partial or Unsatisfactory ratings should have comments to explain your finding and a recommended mitigation.

The criteria for each rating is listed in the following table. (See TABLE 3: BPATS RATING SYSTEM). An Uncertain rating will be further explained below.

Satisfactory	Partial	Unsatisfactory	Uncertain
Evidence indicates security system has satisfied the BPATS	Evidence indicates most security systems have satisfied the BPATS	Evidence clearly indicates security system has not satisfied the BPATS, or	Unknown
Evidence is credible, coherent and fully understood	Some evidence is credible, coherent and fully understood	Evidence is not credible or not coherent, or	Unknown
Evidence does not have obvious internal inconsistencies or inconsistencies with other evidence	Some evidence does not have obvious internal inconsistencies or inconsistencies with other evidence	There is significant inconsistency in the evidence	Unknown

TABLE 3: BPATS RATING SYSTEM

Note: In field testing of the BPATS Tool, assessors found it difficult to maintain the "Not a compliance drill" goal with a binary Satisfactory / Unsatisfactory system. Therefore, in this field guide and in the BPATS on-line tool the rating categories are expanded to Satisfactory, Partial and Unsatisfactory. Comments are required to explain Partial or Unsatisfactory rating.

An "uncertain" rating applies when the assessor cannot determine from the documentation review or the site visit if the facility security system is comparable to the BPATS under review. This rating is appropriate when more or better information is needed to rate the system "satisfactory", "partial" or "unsatisfactory." For each uncertain rating, the assessor should:

- Identify the degree to which it affects the system's anti-terrorism capability;
- Identify a way to resolve the issue (if possible);
- Assess the impact on the evaluation if the issue is not resolved.;
- Document the missing information in the report.

Assessors will rely on their expertise and experience to rate the capability and effectiveness of the facility security program. Remember the ratings justification must be evidence based. This may be accomplished by any of the following methods:

- Support the rating by referencing documentation, records, observations made during the site visit or by other forms of evidence.
- Reference any common security practices implemented. Be detailed in your explanation.
- List assumptions, if any, made while rating a best practice. Describe any inherent risks associated with those assumptions.
- For "Uncertain" or "Unsatisfactory" ratings, list what other information, if any, is needed to change the rating.

5.3.Report Development

Following the documentation review and site visit, the next step is to complete an assessment report. The purpose of the assessment report is to provide a record of the evaluation of the full scope of the assessment, not generalities. The report should contain the information listed below.

- Executive Summary
- Facility Overview
  - Threat Synopsis
    - General Threats
    - Unique Threats to the Facility
  - Site Details
  - Ownership, Management and Subagents
  - Key Assessment Participants
- Assessment Approach
  - Assessment Date
  - Assessment Scope
  - Assessment Team

- Assessment Findings
  - Document Review
  - Prioritized Consolidated Concerns
  - Consolidated List of Innovative Practices
  - Parts of the Anti-Terrorism Security System Not Assessed
  - Difficulties of Obstacles Encountered
- Confidentiality Agreement
- Signature
- Appendix A: Pictures / Diagrams
- Appendix B: Comprehensive Building Assessment Best Practices for Anti-Terrorism Security (BPATS)

Four areas to highlight with additional guidance are the Assessment Team entry, the Executive Summary the Assessment Worksheets, and Lessons Learned.

5.3.1. Assessment Team

Assessments carried out by an independent, experienced and knowledgeable assessor(s) may enhance the significance given to an assessment. Assessors are encouraged to include a copy of their resume in the report.

Evidence of an experienced and knowledgeable assessor may include four years of progressive experience in the physical security field and a bachelor's degree or higher from an accredited institution of higher education or completion of a building security professional certification program such as those offered by ASIS International, the Building Owners and Managers Institute International, or other professional societies. (i.e. Physical Security Professional (PSP), or Certified Protection Professional (CPP). Assessors should also have experience / training relevant to the seven knowledge domains of the Best Practices for Anti-Terrorism Security (BPATS).

For assessments using the online BPATS Based Assessment Tool, it has a place to include the assessor's qualifications. The tool includes the Professional Summary, Education, Training, & Certifications, and Completion Date of BPATS Based Assessment Tool training.

5.3.2. Executive Summary

The purpose of the Executive Summary is to provide the reader with a brief but comprehensive overview of the report's key findings on the facility security program's anti-terrorism capability. It should include the overall ratings and findings of the 24 BPATS as well as observations and comments of those ratings. The Executive Summary should include notable strengths or positive aspects of the facility's security. Finally, the Executive Summary should include any major difficulties or obstacles that were encountered during either the document review or the site visit.

5.3.3. Assessment Worksheets

In the recommended report outline, worksheets covering the 24 BPATS and the 411 Common Security Practices are included as an appendix. Each Worksheet includes an overall BPATS rating (Satisfactory, Partial, Unsatisfactory, Uncertain), summary comments on documentation, Common Security Practices, and observations of the BPATS, comments on assumptions, and comments on "Uncertain" or "Unsatisfactory" BPATS ratings. The worksheets also include an Observation and Recommendation for each Common Security Practice not rated "Satisfactory".

These sheets make up the main bulk of the assessment report.

5.3.4. Lessons Learned

The following Lessons Learned were developed through discussions with the OSAI concerning assessment reports.

- One of the first things to remember is that you shouldn't try to protect the facility with a perfect report. This type of report lacks credibility, since it is likely that most facilities will have some areas that can be improved upon. Findings may be corrected in the next step, when the Owner/Operator develops and executes a mitigation plan.
- All assessments need to be based on solid, credible evidence that stems from the documentation review and site visit. Be specific, not general.
- Also remember that the assessment ratings are not "all or nothing" for the entire site. There may be parts of the facility that are better protected then others. For example, a facility's main tower may have significantly more layers of security than a commercial plaza.
- When it comes to writing the report, stick to just the facts; don't include any marketing information or content not directly relevant to the assessment.
- Finally, highlight Assessor Credentials in the report.

5.3.5. Routing of Reports

If there is a terrorist incident, injured parties may request access to assessment reports to see if terrorists exploited a weakness that had been previously identified. Written records of a security assessment can be viewed as a double-edged sword. No records or poor records may make it difficult for a facility to credibly assert that it regularly assessed its security program and mitigated findings. However, an assessment program coupled with a mitigation strategy may show a stronger due diligence by the Owner.

You should also recognize that not all information is treated the same. There may be confidential business information or privileged information and Personally Identifiable Information (PII) that may require special steps to protect. For building owners/operators that submit SAFTEY Act applications to OSAI, documents provided in support of those applications will be treated as SAFETY Act Confidential Information (SACI). Those protections do not apply to the assessment copy sent to and held by the Building Owner / Operator.

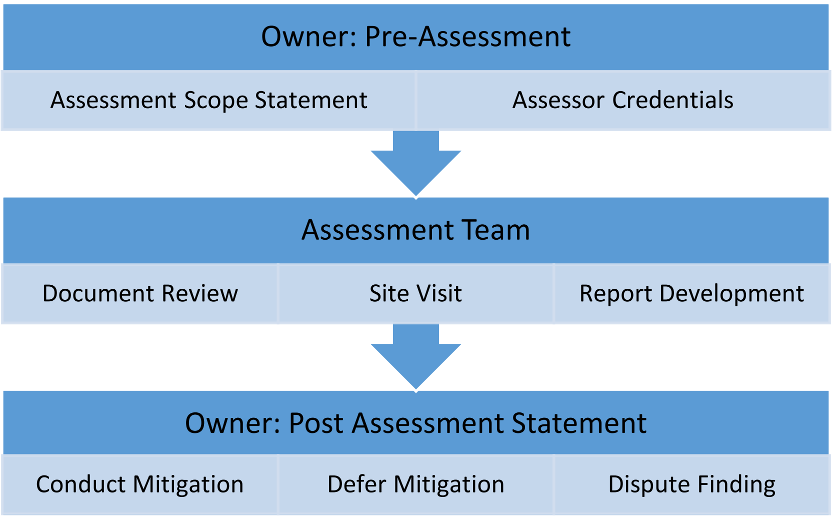
As part of the Report Phase, coordinate with the owner/operator to identify their information protection policies and routing instructions for the assessment documents. For example, they may have you pass information to their General Counsel.

Note: The Assessment report is just one part of a SAFETY Act application. The use of the BPATS tool and assessment results help building owners take the first steps in preparing an application for SAFETY Act protections, should the building owner wish to apply.

6. Owner/Operator Actions

Owner/Operator actions include establishing an assessment scope statement, selecting an assessment team, supporting the assessment and post assessment analysis / mitigation / documentation.

The following diagram depicts the process (*See Diagram 3: ASSESSMENT PROCESS*):



Owner: Pre-Assessment

Assessment Scope Statement | Assessor Credentials

Assessment Team

Document Review | Site Visit | Report Development

Owner: Post Assessment Statement

Conduct Mitigation | Defer Mitigation | Dispute Finding

DIAGRAM 3: ASSESSMENT PROCESS

6.1. Post Assessment Actions: Mitigation, Deferred Mitigation, Acceptance of Risk

After the assessment is completed and submitted to the Owner, the next step is analysis and mitigation decision-making: Mitigation, Deferred Mitigation, Acceptance of Risk.[1]

In the assessment report, the owner is provided assessment findings including:

- Document Review
- Prioritized Consolidated Concerns
- Consolidated List of Innovative Practices
- Parts of the Anti-Terrorism Security System Not Assessed
- Difficulties of Obstacles Encountered

Each of these findings should be addressed in a post assessment mitigation / risk acceptance summary. This records the owners post assessment actions:

- Analysis and evaluation of the risk associated with each finding

[1] For a detailed discussion on incremental protection for existing commercial buildings see FEMA publication "*Risk Management Series, Incremental Protection for Existing Commercial Buildings from Terrorist Attack. Providing Protection to People and Buildings*". FEMA 459 / April 2008

- Determination of appropriate ways to eliminate the hazard, or control risk if the hazard cannot be eliminated
- Completion of mitigation actions
- Deferred mitigation
- Re-evaluation of each finding after mitigation based on compliance with mitigation decisions

Where owners decide to defer mitigation, or take no action following appropriate risk analysis or for other reasons, it is recommended that those decisions are reviewed by the senior management body of the organization and a formal minute is recorded of both the decision reached and the reasons for reaching it.

Note: The BPATS and CSP lists are not intended to be used as rigid decision-making criteria to declare a facility 'safe' or 'not safe' from terrorism solely based on a single finding. The use of the BPATS tool and assessment results help building owners take the first steps in preparing an application for SAFETY Act protections, should the building owner wish to apply.

6.2.Recording Post Assessment Actions in the BPATS Tool

An Owner level user account in the BPATS assessment tool allows the owner to import the encrypted assessment file, view the assessment section by section as well as in five report formats, enter comments on each finding in the document review section and the BPATS section and make general comments on other aspects of the assessment. The Owner can then produce a report summarizing the owner's actions and the resulting improvement to the status of the facility. This is called the "Consolidated List of Owner/Representative Comments" report.

Steps to use the BPATS Tool to record Owner actions:

1. The Owner establishes an Owner level user account and gives the assessor their account code.
2. The Assessor grants access to the assessment to the Owner in the system.
3. Owner receives the encrypted assessment file form the assessor.
4. The Owner logs in to the BPATS Tool and imports the encrypted assessment file.
5. The Owner views the assessment section by section or prints out the findings and uses the list to facilitate planning for Mitigation or Deferred Mitigation / Acceptance of Risk. The owner may also enter a "Disputed" rating and provide comments on uncertainties or missing information that would contradict an assessor's finding.
6. The Owner conducts mitigation.
7. The Owner records Mitigation, Deferred Mitigation / Acceptance of Risk or disputed rating comments on each finding in the document review section, the BPATS section and the Summary section of the assessment in the report titled: Consolidated List of Owner/Representative Comments.

6.3. Samples of Owner Comments to include operational procedures and technology

Owner comments should reference the BPATS finding, be evidence based and supported by documentation, records and observations made after mitigation. The following are samples of mitigation strategies and Owner comments, to include operational procedures and technology.

- Project how recommended actions improve the situation. For example:

> *Access control to telecommunication room doors was identified in finding 3.2.05 as a weakness. In January XXXX a new XXX brand access control system was established on all telecommunication room doors. A person breaking into a room will now be detected and assessed by the security force. Response procedures have been prepared and coordinate with tenants.*

- Identify the key elements for believing there is or is not justification to take action. For example:

> *Finding 6.1.02 stated that glass should be selected and designed to meet the security requirements of the threat(s), threat locations and vulnerabilities identified in the site risk assessment. Based on this finding, a risk assessment, was conducted by XXX on XX/XX/XXXX. The assessment determined the highest risk was to the conference room windows facing XXX street due to their proximity to the street and that they overlook a mass gathering area. (See attached Risk Assessment XXXX). These windows were fitted with fragment retention films on XX/XX/XXXX to mitigate the greatest risk. (See project description in attachment XXX.)*

- Identify key uncertainties and what additional information could reduce the uncertainties. For example*:*

> *Information on the training status of the security force was not available to the assessor during the assessment period. On XX/XX/XXXX the Security Force contractor supplied a training report for the status of the Security force. All personnel were found in compliance.*

- Identify newly implemented security technologies. For example:

The control of master keys to the utility rooms and perimeter doors was a weakness in the assessment report, BPATS 2.3.20. An electronic key box system has been established for the cleaning crew and all utility and perimeter door locks have been reconfigured with a smart key system.