APPENDIX B
DEPARTMENT OF THE INTERIOR FACILITY SECURITY STANDARDS

1. Introduction

The day after the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the President directed the Department of Justice to assess the vulnerability of Federal office buildings in the United States, particularly to acts of terrorism and other forms of violence. Prior to the study, there were no government-wide standards for security at Federal facilities, and no central database of the security currently in place in such facilities.

In the aftermath of the events on September 11, 2001, the Department of the Interior (DOI) has reviewed and upgraded the minimum building/facility standards (for Department of Interior owned and leased facilities) previously established by the U.S. Department of Justice. The Department must carry on its mission while providing heightened security and safety at a wide variety of buildings, monuments, dams, and other facilities. In addition, it is vitally important that all employees remain vigilant, prepared, and ready to protect themselves, their co-workers, and facilities and to deter terrorist attacks.

As stated in the Homeland Security Advisory System document, "The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks."

1.1 The Development of Recommended Minimum Security Standards

The Office of Law Enforcement and Security (OLES) along with representatives from all Interior Bureaus, the U.S. Department of Justice (including the Federal Bureau of Investigation), the U.S. Secret Service, FPS, State Department, and Department of Defense have conducted security surveys at numerous Department of the Interior structures to include Critical Infrastructures and Key Assets. Based upon these past and current security reviews, OLES has identified and evaluated various types of security measures which could be used to counter potential vulnerabilities.

The product of OLES's work is a set of minimum standards that can be applied to various Interior facilities. The standards cover the subjects of security personnel, perimeter, entry, and interior security, and security planning. They are set out in Attachment 1, Facility Security Standards Chart.

Because of the considerable differences among Interior facilities and their security needs, four separate security categories were developed to determine which minimum standards are appropriate for which level of security. The four categories are based on the following factors: total number of DOI employees working at the facility, multi-agency risk considerations, volume of public contact, amount of localized crime, production or development of critically sensitive and/or classified information or projects, storage of biological/chemical/radiological or other hazardous agents, economic/social impact resulting from a loss of the facility, effect this facility

could have resulting in other catastrophes, and location of critical systems in the facility. The categories range from Level I (typically, leased space with ten or fewer employees) to Level IV (typically with greater than 450 employees). Attachment 1 lists the recommended minimum-security standards applicable to each security level. Attachment 2 provides a detailed description of each standard.

2. Defining the Minimum Security Standards

Ninety-one (91) security standards were developed for Interior facilities. The standards are listed in Attachment 1 and are further described in Attachment 2. They fall into the following categories.

2.1 Security Personnel

Security personnel standards refer to the desired location, type, and equipment used by facility security personnel and information regarding other law enforcement that may work in the facility.

The elements of security personnel are:

- Facility Security Personnel
- Other Law Enforcement in Facility

2.2 Perimeter Security

Perimeter security standards pertain to the areas outside of the facility and therefore may extend outside of government control. Depending on the facility type, the perimeter may include sidewalks, parking lots, outside walls of the facility, a hallway, or simply an office door.

The elements of perimeter security are:

- Parking
- Closed Circuit Television Monitoring
- Lighting
- Physical Barriers

2.3 Entry Security

Entry security standards refer to security issues related to the entry of persons and packages into a facility.

The elements of entry security are:

- Receiving/Shipping
- Access Control
- Entrances/Exits

2.4 Interior Security

Interior security standards refer to security issues associated with prevention of criminal or terrorist activity within the facility. This area concerns secondary levels of control after people or items have entered the facility.

The elements of interior security are:

- Employee/Visitor Identification
- Utilities
- Occupant Emergency Plans
- Day Care Centers
- Cyber Issues
- Fire Rescue/Life Safety

2.5 Security Planning

Security planning standards refer to recommendations requiring long-term planning and commitment, as well security standards addressing broader issues with implications beyond security at a particular facility.

The elements of security planning are:

- Intelligence Sharing
- Training
- Tenant Assignment
- Administrative Procedures
- Construction/Renovation

3. Security Levels for Department of the Interior Facilities

Since there are vast differences in types of Interior facilities and their security needs, the facilities were divided into four security levels (levels I – IV). The four security levels are described below.

The listed security levels have been based on ten separate criteria. Final assignment of a security level to a facility will be adjusted based on designation, threat intelligence, crime statistics, agency mission, etc.

Level I

- The total number of DOI employees working at the facility is less than 11.
- The facility/location does not have multi-agency risk considerations.
- The facility has a low volume of public contact.

- The facility is not located in a significant crime area.
- The occupants of the facility do not produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility does not have a laboratory or storage area containing biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be minimal.
- The loss of this facility would not cause or be a factor in other catastrophes.
- The facility/structure does not contain Bureau/Office critical systems.
- The facility/structure has not been designated as a "Critical Infrastructure/Key Asset."

Level II

- The total number of DOI employees working at the facility is between 11 and 150.
- The facility/location does not have multi-agency risk considerations.
- The facility has a moderate volume of public contact.
- The facility is not located in a significant crime area.
- The occupants of the facility do not produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility may have a laboratory or storage area containing a small amount of biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be at a localized level.
- The loss of this facility would not be a determining factor of other catastrophes.
- The facility/structure does not contain Bureau/Office critical systems.
- The facility/structure has not been designated as a "Critical Infrastructure/Key Asset."

Level III

- The total number of DOI employees working at the facility is between 151 and 450.
- The facility/location may have multi-agency risk considerations.
- The facility has a moderate to significant amount of public contact.
- The facility may be located in a significant crime area.
- The occupants of the facility may produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility may have a laboratory or storage area containing a moderate amount of biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be at a regional level.
- The loss of this facility may be a factor in other catastrophes.
- The facility/structure does not contain Bureau/Office critical systems.

- The facility/structure has not been designated as a "Critical Infrastructure/Key Asset."

Level IV

- The total number of DOI employees working at the facility is greater than 450.
- The facility/location may have multi-agency risk considerations.
- The facility has a significant amount of public contact.
- The facility may be located in a significant crime area.
- The occupants of the facility produce or develop critically sensitive and/or classified information or projects on a regular basis.
- The facility has a laboratory or storage area containing a significant amount of biological/chemical/radiological or other hazardous agents (that are not commercially available to the general public).
- The economic/social impact caused by the loss of this facility by the government/private sector would be at a national level.
- The loss of this facility could cause or be a factor in other catastrophes.
- The facility/structure may contain Bureau/Office critical systems.
- The facility/structure has not been designated as a "Critical Infrastructure/Key Asset."

4. Application of Recommended Minimum Security Standards to Security Levels of Interior Facilities

The recommended minimum-security standards applicable to each of the four security levels are covered in Attachment 1, Facility Security Standards Chart. A detailed description of each standard is set out in Attachment 2, Details of Recommended Security Standards.

Appendix B, Attachment 1

FACILITY SECURITY STANDARDS CHART

M - MINIMUM STANDARD
S - STANDARD BASED ON FACILITY EVALUATION
D – DESIRABLE
N/A - NOT APPLICABLE

FACILITY LEVEL	I	II	III	IV
SECURITY PERSONNEL	.	.	.	.
FACILITY SECURITY PERSONNEL	.	.	.	.
Posts at all accessible entrances/exits	N/A	D	S	M
Roving Patrols	N/A	D	S	M
Armed Officers at all Magnetometer Screening Checkpoints	M	M	M	M
24 Hour Presence	N/A	D	M	M
Access to EOD K-9 Unit on a 24 Hour Basis	D	D	D	M
Designated Counter Surveillance Unit	N/A	N/A	D	S
Reliable 24 Hour Communication System for All Security Personnel	D	D	S	M
Interoperable Communications System With Other Organizations	D	D	D	S
Fixed Posts with 360 Degree Coverage	N/A	N/A	D	S
Dedicated Armed Security Presence	N/A	D	D	M
Dedicated Trained On Site Security Manager	N/A	D	D	S
OTHER LAW ENFORCEMENT IN FACILITY	.	.	.	.
Name, Contacts and Working Hours of Other Law Enforcement in the Facility	M	M	M	M
PERIMETER SECURITY	.	.	.	.
Secure Exterior Utility Systems, HVAC Systems, and Vulnerable Fuel Sources	N/A	D	S	M
PARKING	.	.	.	.
Control of Facility Parking	D	D	M	M
Control of Adjacent Parking (If Achievable)	D	D	D	S
Screen All Vehicles Within 100 Feet (If Achievable)	D	D	D	S
Avoid Leases Where Parking Cannot be Controlled	D	D	D	S
Post Signs and Arrange for Towing Unauthorized Vehicles	S	S	M	M
ID System and Procedures for Authorized Parking (Placard, Decal, Card Key, etc.)	D	D	M	M
Adequate Lighting for Parking Areas	D	S	M	M
Employee Parking Separated From Public Parking (If	D	D	S	M

Achievable)				
Bollards (other barriers) Preventing Unauthorized Access	D	D	D	M
CLOSED CIRCUIT TELEVISION (CCTV) MONITORING	.	.	.	.
CCTV Surveillance Cameras With Time Lapse Video Recording, Pan Tilt and Zoom Capability, Still Picture Capability, 360 Degree Coverage, with a Back-up Power Supply	D	S	S	M
Security Room with Two Officers Monitoring the CCTV System on a 24-Hour Basis	D	D	S	M
One Monitor for Every Eight Cameras	D	D	D	D
LIGHTING	.	.	.	.
Exterior Lighting with 360 Degree Coverage Around the Facility	S	S	S	M
Parking Area Lighting	D	D	D	S
Exterior/Interior Lighting with Emergency Power Backup	M	M	M	M
Lighting Meets Minimum for the CCTV System	M	M	M	M
PHYSICAL BARRIERS	.	.	.	.
Extend Physical Perimeter with Rated or Landscape Barriers (If Achievable)	N/A	N/A	D	S
Rated or Landscape Barriers Separating Drop Off/Parking Area from the Facility	N/A	N/A	D	S
ENTRY SECURITY	.	.	.	.
RECEIVING/SHIPPING	.	.	.	.
Review/Implement Receiving/Shipping Procedures	M	M	M	M
Restrict Delivery Access to Authorized Personnel/Vehicles	D	D	S	M
Post, Monitor or Secure Receiving/Shipping Areas	D	D	S	M
X-Ray All Incoming Packages	D	D	S	M
Irradiate All Incoming Mail	D	D	S	S
Security Training for Mailroom Personnel	D	D	S	M
ACCESS CONTROL	.	.	.	.
Card Key or Similar System to Record Entry/Exit Times	D	D	S	S
Security Personnel Posted at all Open Access Points Checking Identification	D	D	S	M
Intrusion Detection System (IDS) with 24-Hour Central Monitoring Capability	D	S	M	M
IDS Utilizing Line Supervision and Backup Power	D	D	S	M
IDS Covering all Access Points	D	S	S	M
Central Database Containing the Location and Serial Number of all Keys	S	S	S	M
ENTRANCES/EXITS	.	.	.	.
X-Ray and Magnetometer at Public Entrances with	N/A	D	S	M

Trained Operators				
Require X-Ray Screening of All Packages	N/A	D	S	M
Radiation Screening Device	N/A	D	D	S
Peep Holes	S	S	N/A	N/A
Intercom	S	S	N/A	N/A
Entry Control w/CCTV and Door Strikes	D	S	N/A	N/A
Post Signs Advising of 24 Hour Video Surveillance (if CCTV system in use)	M	M	M	M
High Security Locks	M	M	M	M
Door Hinges Located on the Inside	M	M	M	M
Secure Doors/Set Alarms on Off Hours	M	M	M	M
INTERIOR SECURITY	.	.	.	.
EMPLOYEE/VISITOR IDENTIFICATION	.	.	.	.
Agency Photo ID for all Personnel Displayed at all Times	N/A	D	S	M
Visitor Control System	D	M	M	M
Visitor Identification Accountability System	N/A	D	S	M
Establish Identification Issuing Authority	S	S	S	M
UTILITIES – INCLUDING HVAC	.	.	.	.
Prevent Unauthorized Access to Utility Areas	S	S	M	M
Provide Emergency Power to Critical Systems (Alarm Systems, Radio Communications, Computer Facilities, etc.)	M	M	M	M
Ability and Procedures to Close Air Intake System	D	D	S	S
Dedicated HVAC systems for lobbies, mailrooms, and loading docks	D	D	D	S
OCCUPANT EMERGENCY PLANS	.	.	.	.
Examine, Update and Practice Occupant Emergency Plans (OEP) and Contingency Procedures Based On Threats	M	M	M	M
Contacts for Local Police, Fire Department, HAZMAT Teams, EOD Team, etc.	M	M	M	M
Assign and Train OEP Officials (Assignment Based on Largest Tenant in the Facility)	M	M	M	M
Annual Tenant Training	M	M	M	M
Establish Relocation Primary and Secondary Sites	M	M	M	M
DAYCARE CENTERS	.	.	.	.
Evaluate Whether to Locate Daycare Centers in Federal Facilities	N/A	M	M	M
Review Location, Access, Evacuation, Drop-off/Pick-up Procedures Once Per Year	N/A	M	M	M
CYBER ISSUES	.	.	.	.
All Official Computers in Compliance with Current DOI Security Standards	M	M	M	M
“Stand Alone” Computers in Control of Vital Systems	D	D	D	D

Back-up Power Supply for Computers Monitoring Security/Vital Systems	D	D	S	M
FIRE RESCUE/LIFE SAFETY	.	.	.	.
Presence of a Facility Emergency Public Address System	D	D	S	M
Establish “Shelter In Place” Plan (where appropriate)	M	M	M	M
SECURITY PLANNING	.	.	.	.
INTELLIGENCE SHARING	.	.	.	.
Establish Law Enforcement Agency/Security Liaison	M	M	M	M
Review/Establish Procedure for Intelligence Receipt/Dissemination	M	M	M	M
Establish “in office” Unusual Facility Incident Reporting System	M	M	M	M
TRAINING	.	.	.	.
Conduct Annual Security Awareness Training (Including Chemical/Biological/Radiological)	M	M	M	M
Establish Standardized Unarmed Guard Qualifications/Training Requirements	M	M	M	M
Establish Standardized Armed Guard Qualifications/Training Requirements	M	M	M	M
TENANT ASSIGNMENT	.	.	.	.
Co-Locate Agencies With Similar Security Needs	D	D	D	D
Do Not Co-Locate High/Low Risk Agencies	D	D	D	D
ADMINISTRATIVE PROCEDURES	.	.	.	.
Review Guidelines to Establish Flexible Work Schedule in High Threat/High Risk Areas to Minimize Employee Vulnerability to Criminal Activity	S	S	D	D
Arrange for Employee Parking In/Near Facility After Normal Work Hours	S	S	S	S
Establish Security Control Procedures for Service Contract Personnel	M	M	M	M
CONSTRUCTION/RENOVATION	.	.	.	.
Install Mylar Film on Exterior Windows (Shatter Protection)	D	D	S	M
Review Current Projects for Blast/Natural Disaster Standards	M	M	M	M
Review/Establish Uniform Standards for Construction	M	M	M	M
Review/Establish New Design Standard for Blast Resistance	S	S	M	M
Review Appropriateness of Installing Vehicle Barriers	D	S	M	M
Establish Street Set-Back When Possible for New Construction	D	D	S	M
Review Current Projects for Fire Safety Code	M	M	M	M

Appendix B, Attachment 2

DETAILS OF RECOMMENDED SECURITY STANDARDS

Security Personnel	
Term	**Definition/Description**
FACILITY SECURITY PERSONNEL	…….
POSTS AT ALL ENTRANCES/EXITS	All accessible entrance/exits, will have stationed security personnel adhering to entrance/exit protocol.
SECURITY FIXED POST	A fixed area of responsibility designated for observation, screening or performing information gathering by security personnel. Security personnel will only deviate from this location when they are relieved or in a critical emergency situation (i.e. fire, etc.).
ROVING PATROLS	Geographic areas designated for general observation, response or performing information gathering by security personnel. Security personnel will only deviate from the patrol area when they are relieved or in a critical situation.
ARMED OFFICERS AT ALL MAGNETOMETER SCREENING CHECK POINTS	A percentage of the security force should be authorized to carry firearms. At a minimum, these personnel should be positioned at all screening areas, on roving patrols, and in the response mode.
24-HOUR PRESENCE	The security force should maintain a constant presence at the facility.
ACCESS TO EOD K-9 UNIT ON A 24-HOUR BASIS	Ability to contact and summon an explosive ordinance division dog to assist in suspicious package identification.
COUNTER SURVEILLANCE UNIT	Security personnel in an “under-cover” roving patrol observing possible vulnerabilities and gathering information. The personnel remain in contact with the control room and only respond and identify themselves in exigent circumstances.
RELIABLE 24-HOUR COMMUNICATION SYSTEM	A communication system issued to all security personnel with a minimal amount of “dead” spots that is monitored on a 24-hour basis.
INTEROPERABLE COMMUNICATION SYSTEM WITH OTHER	A reliable 24-hour communications system that can be monitored/used by other law

Security Personnel	
ORGANIZATIONS	enforcement organizations.
360 DEGREE COVERAGE	Security posts positioned to effectively eliminate any non-screened/observed individual from entering a secure area.
DEDICATED TRAINED ON SITE SECURITY MANAGER	A Security Manager who has completed Security Training at FLETC or other accredited Security Managers Course.
OTHER LAW ENFORCEMENT IN FACILITY	……..
NAME, CONTACTS, AND WORKING HOURS OF OTHER LAW ENFORCEMENT IN FACILITY	Maintain liaison contact for intelligence issues, emergency response, etc.

Perimeter Security	
Term	**Definition/Description**
PARKING	…….
SECURE EXTERIOR UTILITY SYSTEMS, HVAC SYSTEMS, AND VULNERABLE FUEL SOURCES	Exterior utility systems should be assessed for possible vulnerabilities and appropriate measures should be taken.
CONTROL OF FACILITY PARKING	Access to government parking should be limited where possible to government vehicles and personnel. At a minimum, authorized parking spaces and vehicles should be assigned and identified.
CONTROL OF ADJACENT PARKING	Where feasible, parking areas adjacent to Federal space should also be controlled to reduce the potential for threats against Federal facilities and employee exposure to criminal activity.
SCREEN ALL VEHICLES WITHIN 100 FEET	All vehicles entering a perimeter of 100 feet of the facility should be visually or K-9 searched.
AVOID LEASES WHERE PARKING CANNOT BE CONTROLLED	Endeavor to negotiate guard services as part of the lease.
POST SIGNS AND ARRANGE FOR TOWING UNAUTHORIZED VEHICLES	Procedures should be established and implemented to alert the public to towing policies and the removal of unauthorized vehicles.
ID SYSTEM AND PROCEDURES FOR AUTHORIZED PARKING	Procedures should be established for identifying vehicles and corresponding parking spaces. (Placard, decal, card key, etc.)
ADEQUATE LIGHTING FOR PARKING	Effective lighting provides added safety for

Perimeter Security	
AREAS	employees and deters illegal or threatening activities.
EMPLOYEE PARKING SEPERATED FROM PUBLIC PARKING	Segregating the parking allows for different levels of screening.
BOLLARDS PREVENTING UNAUTHORIZED ACCESS	Barriers (bollards, landscaping, etc.) should be strategically positioned around the facility to increase the standoff distance of unauthorized vehicles.
CLOSED CIRCUIT TELEVISION (CCTV) MONITORING	……
CCTV SURVEILLANCE CAMERAS WITH TIME LAPSE VIDEO RECORDING, PTZ CAPABILITY, STILL PICTURE CAPABILITY, 360 DEGREE COVERAGE, WITH A BACK-UP POWER SUPPLY	Twenty-four hour CCTV surveillance and recording is desirable at all locations as a deterrent. Requirements will depend on assessment of the security level for each facility. Time-lapse video recordings/still pictures are also highly valuable as a source of evidence and investigative leads.
SECURITY ROOM WITH TWO OFFICERS MONITORING THE CCTV SYSTEM ON A 24-HOUR BASIS	Security cameras have been used to decrease the manpower needed in certain areas. Cameras are only effective when they are being monitored.
ONE MONITOR FOR EVERY EIGHT CAMERAS	Eight is about the maximum number of cameras that can effectively cycle through one monitor.
LIGHTING	……..
EXTERNAL LIGHTING WITH 360 DEGREE COVERAGE	All attempts should be made to minimize any "dark" spots near or adjacent to any facility.
PARKING AREA LIGHTING	Employee parking areas require adequate illumination.
EXTERIOR/INTERIOR LIGHTING WITH EMERGENCY POWER BACKUP	Standard safety code requirement in virtually all areas. Provides for safe evacuation of facilities in case of natural disaster, power outage or criminal/terrorist activity.
LIGHTING MEETS MINIMUM FOR THE CCTV SYSTEM	The CCTV monitoring system will not be effective without proper illumination.
PHYSICAL BARRIERS	……..
EXTEND PHYSICAL PERIMETER WITH RATED OR LANDSCAPE BARRIERS (IF ACHIEVABLE)	This security measure will only be possible in locations where the Government controls the property and where physical constraints are not present. (Barriers of concrete, steel, trees, boulders, earthen walls, etc.)
RATED OR LANDSCAPE BARRIERS	Desirable to prevent unauthorized vehicle

Perimeter Security	
SEPARATING DROP OFF/PARKING AREA FROM FACILITY	access into the parking area and from the parking area to the facility.

Entry Security	
Term	**Definition/Description**
RECEIVING/SHIPPING	……..
REVIEW/IMPLEMENT RECEIVING/SHIPPING PROCEDURES	Audit current standards for package entry, suggest ways to enhance security, and implement improved procedures.
RESTRICT DELIVERY ACCESS TO AUTHORIZED PERSONNEL/VEHICLES	Unauthorized passenger or other vehicles should not be allowed access to park, drop-off passengers or "stand" in the loading area.
POST, MONITOR OR SECURE RECEIVING/SHIPPING AREAS	See "Security Post" and "CCTV" definitions. Secure (lock) the area when not in use.
X-RAY ALL INCOMING PACKAGES	In an attempt to detect an explosive, incendiary device, weapon, etc.
IRRADIATE ALL INCOMING MAIL	In an attempt to render safe a biological devise
SECURITY TRAINING FOR MAILROOM PERSONNEL	All Mailroom personnel should have yearly training regarding the detection and mitigation of hazardous substances/devices.
ACCESS CONTROL	…….
CARD KEY OR SIMILAR SYSTEM TO RECORD ENTRY/EXIT TIMES	Prevents unauthorized entry and keeps a current database of who is located in the facility and usage of the facility on different days and times.
SECURITY GUARD POSTED AT ALL OPEN ACCESS POINTS CHECKING IDENTIFICATION	See "Security Post."
INTRUSION DETECTION SYSTEM (IDS) WITH 24-HOUR CENTRAL MONITORING CAPABILITY	A basic, cost effective security measure.
IDS USING LINE SUPERVISION AND BACKUP POWER	An IDS system that is activated if the main reporting line is interrupted (i.e. phone line is cut) and is not affected by power fluctuations.
IDS COVERING ALL ACCESS POINTS	All possible entrances/exits into the facility should be covered by this system, not just key locations.
CENTRAL DATABASE CONTAINING THE LOCATION AND SERIAL	The integrity of the locking system must be maintained.

Entry Security	
NUMBER OF ALL KEYS	
ENTRANCES/EXITS	……
X-RAY AND MAGNETOMETER AT PUBLIC ENTRANCES WITH TRAINED OPERATORS	These devices, although an excellent visual deterrent, will only be truly effective if operated by trained personnel.
REQUIRE X-RAY SCREENING OF ALL MAIL/PACKAGES	All packages entering facility should be subject to x-ray screening and/or visual inspection.
RADIATION SCREENING	For use in level IV and Critical Infrastructures/Key Asset facilities.
PEEP HOLES	Easy and effective visual recognition system for small offices.
INTERCOM	Communication tool that can be used in combination with peephole.
ENTRY CONTROL WITH CCTV AND DOOR STRIKES	Provides employees with the ability to view and communicate remotely with visitors before allowing access. Not applicable for facilities requiring screening devices.
POST SIGNS ADVISING OF 24-HOUR VIDEO SURVEILLANCE	Warning signs advising of 24-hours surveillance act as a deterrent in protecting employees and facilities.
HIGH SECURITY LOCKS	Any exterior entrance should have a high security lock as determined by FPS specifications and/or agency requirements.
DOOR HINGES LOCATED ON THE INSIDE	Basic security measure.
SECURE DOORS/SET ALARMS ON DURING SECURE HOURS	Any security system is ineffective if not operated properly.

Interior Security	
Term	**Definition/Description**
EMPLOYEE/VISITOR IDENTIFICATION	……
AGENCY PHOTO ID FOR ALL PERSONNEL DISPLAYED AT ALL	May not be required in smaller facilities.

Interior Security	
TIMES	
VISITOR CONTROL/SCREENING SYSTEM	Facilities should develop a method to have visitors sign-in and may require an escort or formal identification/badge.
VISITOR ID ACCOUNTABILITY SYSTEM	Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.
ESTABLISH ID ISSUING AUTHORITY	Develop procedures and establish authority for issuing employee and visitor IDs.
UTILITIES	……..
PREVENT UNAUTHORIZED ACCESS TO UTILITY AREAS	Smaller facilities may not have control over utility access, or locations of utility areas. Where possible, assure utility areas are secure and only authorized personnel can gain entry.
PROVIDE EMERGENCY POWER TO CRITICAL SYSTEMS	Tenant agency is responsible for determining which computer and communication systems require back-up power. All alarm systems, CCTV monitoring devices, fire detection systems, entry control devices, etc., require emergency power sources.
ABILITY AND PROCEDURES TO CLOSE AIR INTAKE SYSTEM	Essential to a "shelter in place" plan. Facility Managers should assess and decrease the vulnerability of their facility HVAC system against a Chemical, Biological, and Radiological (CBR) threat.
DEDICATED HVAC SYSTEMS FOR LOBBIES, MAILROOMS. AND LOADING DOCKS	Separate HVAC systems will prevent the contamination of one vulnerable area being spread throughout other areas in the facility.
OCCUPANT EMERGENCY PLANS	……..
EXAMINE OCCUPANT EMERGENCY PLAN (OEP) AND CONTINGENCY PROCEDURES BASED ON THREATS	Review and update current OEP procedures for thoroughness. OEP's should reflect the current security climate.
CONTACTS FOR LOCAL POLICE, FIRE DEPARTMENT, HAZMAT TEAMS, EOD TEAM, ETC.	Contact list should be kept in an accessible area and updated once per year.
ASSIGN AND TRAIN OEP OFFICIALS	Assignment based on GSA requirement that largest tenant in facility maintain OEP

Interior Security	
	responsibility. DOI officials should be assigned, trained, and contingency plan established to provide for the possible absence of OEP officials in the event of emergency activation of the OEP.
ANNUAL TENANT TRAINING	All tenants should be aware of their individual responsibilities in an emergency situation.
ESTABLISH RELOCATION PRIMARY AND SECONDARY SITES	All tenants should be aware of the relocation sites.
DAY CARE CENTERS	…….
EVALUATE WHETHER TO LOCATE DAYCARE CENTERS IN LEVEL III AND IV FACILITIES	Conduct a thorough review of security and safety standards.
REVIEW LOCATION, ACCESS, EVACUTION, DROP-OFF/PICK-UP PROCEDURES ONCE PER YEAR	Daycare Centers should be included in all security assessments.
CYBER ISSUES	…….
ALL OFFICIAL COMPUTERS IN COMPLIANCE WITH CURRENT DOI SECURITY STANDARDS	The CIO's Office should be contacted with any questions/concerns.
"STAND ALONE" COMPUTERS IN CONTROL OF VITAL SYSTEMS	Computers that are not connected to outside systems, i.e. the internet, other DOI systems, etc.
BACK-UP POWER SUPPLY FOR COMPUTERS MONITORING SECURITY/VITAL SYSTEMS	In an effort to negate the power supply as a vulnerability.
FIRE RESCUE/LIFE SAFETY	……..
PRESENCE OF A FACILITY EMERGENCY PUBLIC ADDRESS SYSTEM	A communication system used to transmit emergency information to facility occupants.
ESTABLISH "SHELTER IN PLACE" PLAN	Determine if the facility is acceptable for use during an emergency.

Security Planning	
Term	**Definition/Description**
INTELLIGENCE SHARING	…….
ESTABLISH A SECURITY LIASION OFFICER	At least one Officer should be the liaison contact for other law enforcement agencies.

Security Planning	
	This Officer will be responsible for updating liaison contacts, attending meetings, disseminating information, etc.
REVIEW/ESTABLISH PROCEDURES FOR INTELLIGENCE RECEIPT/DISSEMINATION	Determine what procedures exist to ensure timely delivery and dissemination of critical intelligence. Review and improve procedures to alert agencies and specific targets of criminal and terrorist threats. Establish standard administrative procedures for response to incoming alerts.
ESTABLISH "IN-OFFICE" UNUSUAL FACILITY INCIDENT REPORTING SYSTEM	Provides an historical document for detecting patterns, official record of prior incidents, etc.
TRAINING	……
CONDUCT ANNUAL SECURITY AWARENESS TRAINING (INCLUDING CHEMICAL/BIOLOGICAL/RADIOLOG-ICAL)	Provide security awareness training for all tenants. At a minimum, self-study programs utilizing videos and literature, etc. should be implemented. These materials should provide up-to-date information covering security practices, employee security awareness, and personal safety.
ESTABLISH STANDARDIZED ARMED AND UNARMED GUARD QUALIFICATIONS/TRAINING REQUIREMENTS	Requirements for these positions should be stringently followed.
TENANT ASSIGNMENT	……
CO-LOCATE AGENCIES WITH SIMILAR SECURITY NEEDS	To capitalize on efficiencies and economies, agencies with like security requirements should be located in the same facility if possible.
DO NOT CO-LOCATE HIGH/LOW RISK AGENCIES	Low risk agencies should not take on additional risk by being located with high risk agencies.
ADMINISTRATIVE PROCEDURES	…….
REVIEW GUIDELINES TO ESTABLISH FLEXIBLE WORK SCHEDULE IN HIGH THREAT/HIGH RISK AREA TO MINIMIZED EMPLOYEE VULNERABILITY TO CRIMINAL ACTIVITY.	Flexible work schedules can enhance employee safety by staggering reporting and departure times. As an example, flexible schedules might enable employees to park closer to the facility by reducing the demand for parking at peak times of the day.
ARRANGE FOR EMPLOYEE PARKING IN/NEAR FACILITY AFTER NORMAL WORK HOURS	Minimize exposure to criminal activity by allowing employees to park at or inside the facility.

Security Planning	
ESTABLISH SECURITY CONTROL PROCEDURES FOR SERVICE CONTRACT PERSONNEL	Establish procedures to ensure security where private contract personnel are concerned. Procedures may be as simple as observation or could include sign-in/escort. Frequent visitors may necessitate a background check with contractor ID issued.
CONSTRUCTION/RENOVATION	…….
INSTALL MYLAR FILM ON EXTERIOR WINDOWS (SHATTER PROTECTION)	Application of shatter resistant material to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion.
REVIEW CURRENT PROJECTS FOR BLAST/NATURAL DISASTER STANDARDS	Design and construction projects should be reviewed if possible, to incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards prior to completion of construction.
REVIEW/ESTABLISH UNIFORM STANDARDS FOR CONSTRUCTION	Review, establish, and implement uniform construction standards as it relates to security considerations.
REVIEW/ESTABLISH NEW DESIGN STANDARD FOR BLAST RESISTANCE	In smaller facilities or those that lease space, control over design standards may not be possible. However, future site selections should attempt to locate in facilities that do meet standards. New construction of Government controlled facilities should review, establish, and implement new design standards for blast resistance.
REVIEW APPROPRIATENESS OF INSTALLING VEHICLE BARRIERS	Barriers (various types) may need to be installed to increase “stand-off” distance from the facility.
ESTABLISH STREET SET-BACK FOR NEW CONSTRUCTION	Every foot between a potential bomb and a facility will dramatically reduce damage and increase the survival rate. Street setback is always desirable, but should be used in conjunction with barriers in Level IV facilities.
REVIEW CURRENT PROJECTS FOR FIRE SAFETY CODE	All new projects should be current with all safety codes.