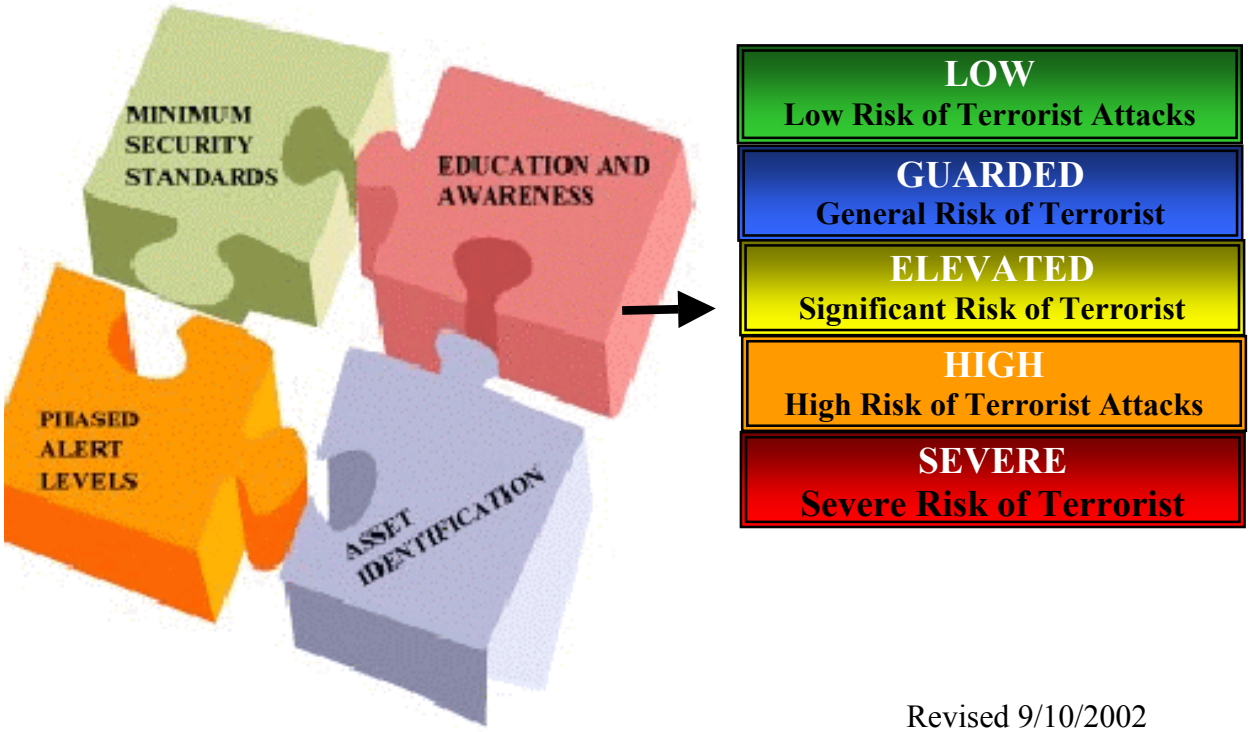
DEPARTMENT OF COMMERCE
OFFICE OF SECURITY

HOMELAND SECURITY GUIDANCE

PHASED FACILITY SECURITY PROGRAM DEVELOPMENT HANDBOOK

HOMELAND SECURITY ADVISORY SYSTEM



Revised 9/10/2002

CONTENTS Page

DEPARTMENT OF COMMERCE

DOJ FEDERAL FACILITY SECURITY LEVEL DETERMINATION
MINIMUM SECURITY STANDARDS AND PHASED SECURITY ALERT SYSTEM

Background

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. Because of its expertise in court security, the United States Marshal Service coordinated the study with the following participating federal agencies: Federal Bureau of Investigation, General Services Administration Federal Protective Service, Department of Defense, U.S. Secret Service, U.S. Department of State, Social Security Administration, and the Administrative Office of the U.S. Courts. Prior to the completion of this study and the issuance of the DOJ Vulnerability Assessment of Federal Facilities Report on June 28, 1995, there were no government-wide minimum standards for security at federal facilities.

The DOJ Vulnerability Assessment of Federal Facilities Report established 52 minimum security standards in five separate security levels (I, II, III, IV, V) with Level V being the highest risk level and Level I the lowest risk level. The DOJ criteria only considered such factors as square footage, tenant population, agency mission sensitivity, and volume of public contact. In the development of the minimum security standards for the five DOJ security levels, the study did not consider agency specific factors such as critical asset protection and essential mission capabilities. Appropriate agency management officials can make adjustments to the assigned risk level based on such factors.

The Department of Commerce (DOC) adopted the DOJ Vulnerability Assessment of Federal Facilities Report and the minimum security standards for federal facilities as the DOC minimum security standards for all DOC controlled facilities. It is the responsibility of DOC senior facility managers to know what their DOJ security level is, to implement the DOJ minimum security standards for their facility, and to evaluate, identify and implement additional security measures based on specific mission and critical asset protection requirements. Between 1996 and 1999, DOC Regional Security Officers (RSO) and Field Security Officers (FSO), in collaboration with DOC facility managers and NOAA's Administrative Support Centers, assigned a DOJ security level for every DOC-controlled facility based on the DOJ security level definitions.

Homeland Security Presidential Directive-3 (PD-3) was issued on March 12, 2002. Homeland Security PD-3 developed a National Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the American people. The Department of Commerce incorporated Homeland Security PD-3 initiatives into the Department's Phased Security Advisory System on June 30, 2002. This system provides warnings in the form of a set of graduated "Threat Conditions" or Alert Levels that would increase as the risk of the threat increases. The DOC Phased Security Advisory System creates a common vocabulary, context, and structure. At each Alert Level, DOC managers and employees will implement their corresponding Phased Security Alert Plan to reduce vulnerability or increase response capability during a period of heightened alert.

The DOC Office of Security recognizes, however, that bringing some facilities up to the DOJ minimum security standards in all areas may not be feasible because of the nature of an existing lease, the unwillingness of a landlord to modify a lease, or a major structural problem. Each facility's security requirements and feasibility of meeting those requirements must be addressed on a building-by-building basis. The DOC/OSY stands committed to provide professional security services to DOC managers to determine individual facility security requirements by providing an Analytical Risk Management Security Survey.

PHASED SECURITY PROGRAM DEVELOPMENT

A. Overview:

To lessen the risk of any incidents or threats to DOC personnel or facilities and to provide a safe and secure environment that is as responsive as practical to mission requirements, appropriate security measures must be developed and correspond to changing threat conditions. The development of phased security procedures provides the DOC bureau and operating unit mangers with the ability to immediately increase their minimum security standards ("Security Alert Level 1,"Low") to a higher level security alert level to manage the risks. Facility managers must know what "Security Alert Low" means at their respective facility. Security contacts, facility managers, or those with responsibility to protect DOC personnel and property are required to develop phased security procedures for their facility. These procedures will be incorporated into the facility Occupant Emergency Plan (OEP) and the Continuity of Operations Plan (COOP).

Minimum security standards range from high security locks on all doors to a 24-hour armed guard force. Each facility manager is required to know the DOJ building security level for his or her facility and the minimum security standards that apply. Based on the facility's DOJ security level, phased security procedures will be developed that tie facility security measures directly to Homeland Security Alert Levels as identified in Homeland Security PD-3. Facility managers have the authority to raise the security alert level of their facility to correspond to local threat conditions or to provide added security measures during periods of potential threat from outside activities or groups, but cannot reduce protective measures set by higher authority. For assistance in applying levels to a particular facility, facility managers should contact their DOC servicing security officer or the DOC Office of Security headquarters.

B. Procedures:

Step 1. DETERMINE DOJ FEDERAL FACILITY SECURITY LEVEL: Each DOC facility must be assessed to determine the building security level based on the DOJ Facility security levels as defined in Appendix A with Level V being the highest risk level and Level I being the lowest. (Currently, the Department of Commerce does not have any Level V facility.) Review the DOJ Facility Security Level definitions below to determine your DOJ facility security level. In most cases, the facility DOJ facility security level was determined during a previous security survey. Contact your servicing security officer for that information and to discuss your determination.

Step 2. IDENTIFY ASSETS TO BE PROTECTED: Identify the assets you want to protect. Assets are normally identified into five categories: People, Facilities, Operational Equipment, Information, and Personal Property. Determine whether each asset is critical or non-critical to the your mission.

Step 3. REVIEW AND EVALUATE THE DOJ FACILITY MINIMUM SECURITY STANDARDS FOR COMPLIANCE AND EFFECTIVENESS: The DOJ report established 52 minimum security standards in the categories of perimeter security, entry security, interior security, and security planning to be considered for a building based on its assessed DOJ security level. In Appendix B, the four tables identify the DOJ minimum security standards that are to be applied to each building on the basis of its designated DOJ facility security level. For example, control of facility parking is recommended as a minimum standard for buildings in security level III through V and recommended as desirable for buildings in security levels I and II.

a. After determining your DOJ Facility Security Level and reviewing the associated DOJ minimum security standards, evaluate each minimum standard for compliance and implement those minimum standards with which your facility is not in compliance.

b. The DOJ minimum security standards may not adequately provide the appropriate level of protection for all your assets. Senior facility managers shall evaluate, identify, and implement additional site-specific minimum security measures as necessary. These additional security measures will become part of your site-specific minimum security standards for your facility and Phased Security Alert Level "Low" in your Phased Security Plan.

Step 4. DEVELOP A PHASED SECURITY ALERT PLAN: Facility managers are required to develop phased security alert procedures for their respective facilities in accordance with Homeland Security PD-3. The guidelines for security alert levels provide a five-tiered set of security measures to be implemented based on your DOJ Facility Security level, minimum security standards, and the nature or degree of the threat. Some actions may be required in a particular facility for specific building security levels and other measures may apply after consultation with the servicing security officer or by the direction of the Director for Security. Sample Phased Security Alert Plans for each DOJ facility security level are provided in Appendix C.

Step 5. INCORPORATE THE PHASED ALERT PLAN INTO THE OCCUPANT EMERGENCY PLAN (OEP): The Phased Security Alert Plan must be incorporated into the facility OEP and become part of the COOP.

Step 6. ESTABLISH AN EDUCATION AND AWARENESS TRAINING PLAN: All assigned facility personnel, both federal and contractors, must be provided training so they fully understand the Phased Security Alert Plan and their individual roles and responsibilities.

Step 7. PROVIDE CONTINUAL REVIEW OF THE PROGRAM: Senior facility managers will review and update their Phased Security Alert Plan annually or sooner as threat, mission, or operational changes dictate.

DOJ VULNERABILITY ASSESSMENT OF FEDERAL FACILITIES
BUILDING SECURITY LEVELS

Definition:

Level V: A building that contains mission functions critical to national security, such as the Pentagon or CIA Headquarters. A Level V building should be similar to a Level IV building in terms of number of employees and square footage. It should have at least the security features of a Level IV building. The missions of Level V buildings require that tenant agencies secure the site according to their own requirements.

Level IV: A building that has more than 450 federal employees; a high volume of public contact; more than 150,000 square feet of space; tenant agencies that may include high-risk law enforcement and intelligence agencies, courts, and judicial offices; and highly sensitive government records.

Level III: A building with 151 to 450 federal employees; moderate/high volume of public contact; 80,000 to 150,000 square feet of space; and tenant agencies that may include law enforcement agencies, court/related agencies and functions, and government records and archives. (According to GSA, at the request of the Judiciary, GSA changed the designation of a number of buildings housing agencies with court and court-related functions from Level III to Level IV.)

Level II: A building that has 11 to 150 federal employees; moderate volume of public contact; 2,500 to 80,000 square feet of space; and federal activities that are routine in nature, similar to commercial activities.

Level I: A building that has 10 or fewer federal employees; low volume of public contact or contact with only a small segment of the population; and 2,500 or less square feet of space, such as a small "store front" type of operation.

Source: Vulnerability Assessment of Federal Facilities, Department of Justice, June 28, 1995.

DOJ FEDERAL FACILITY MINIMUM SECURITY STANDARDS

Table 1: Recommended Minimum Security Standards--Perimeter Security

PERIMETER SECURITY	Facility Security Level				
	I	II	III	IV	V
Parking					
Control of facility parking	D	D	M	M	M
Control of adjacent parking	D	D	D	F	F
Avoid leases in which parking cannot be controlled	D	D	D	D	D
Leases should provide security control for parking	D	D	D	D	D
Post signs and arrange for towing unauthorized vehicles	F	F	M	M	M
ID system and procedures for authorized parking (placard, decal, card key, etc.)	D	D	M	M	M
Adequate lighting for parking areas	D	D	M	M	M
Closed circuit television (CCTV) monitoring					
CCTV surveillance cameras with time lapse video recording	D	F	F	M	M
Post signs advising of 24 hour video surveillance	D	F	F	M	M
Lighting					
Lighting with emergency power backup	M	M	M	M	M
Physical barriers					
Extend physical perimeter with concrete and/or steel Barriers	N/A	N/A	D	F	F
Parking barriers	N/A	N/A	D	F	F

Legend:

Minimum standard = M
Standard based on facility evaluation = F
Desirable = D
Not applicable = N/A

Source: Vulnerability Assessment of Federal Facilities, Department of Justice, June 28, 1995.

Table 2: Recommended Minimum Security Standards--Entry Security

ENTRY SECURITY	Facility Security Level				
	I	II	III	IV	V
Receiving/Shipping					
Review receiving/shipping procedures (current)	M	M	M	M	M
Implement receiving/shipping procedures (modified)	D	F	M	M	M
Access control					
Evaluate facility for security guard requirements	D	F	M	M	M
Security guard patrol	D	D	F	F	F
Intrusion detection system with central monitoring capability	D	F	M	M	M
Upgrade to current life safety standards (fire detection, fire suppression systems, etc.)	M	M	M	M	M
Entrances/Exits					
X-ray and magnetometer at public entrances	N/A	D	F	F	M
Require x-ray screening of all mail/packages	N/A	D	F	M	M
Peepholes	F	F	N/A	N/A	N/A
Intercom	F	F	N/A	N/A	N/A
Entry control with CCTV and door strikes	D	F	N/A	N/A	N/A
High security locks	M	M	M	M	M

Legend:
Minimum standard = M
Standard based on facility evaluation = F
Desirable = D
Not applicable = N/A

Source: Vulnerability Assessment of Federal Facilities, Department of Justice, June 28, 1995.

Table 3: Recommended Minimum Security Standards--Interior Security

INTERIOR SECURITY	Facility Security Level				
	I	II	III	IV	V
Employee/Visitor identification					
Agency photo ID for all personnel displayed at all Times	N/A	D	F	M	M
Visitor control/screening system	D	M	M	M	M
Visitor identification accountability system	N/A	D	F	M	M
Establish ID issuing authority	F	F	F	M	M
Utilities					
Prevent unauthorized access to utility areas	F	F	M	M	M
Provide emergency power to critical systems (alarm systems, radio communications, computer facilities, etc.)	M	M	M	M	M
Occupant emergency plans					
Examine occupant emergency plans (OEP) contingency procedures based on threats	M	M	M	M	M
OEP in place, updated annually, periodic testing Exercise	M	M	M	M	M
Assign & train OEP officials (assignment based on largest tenant in facility)	M	M	M	M	M
Annual tenant training	M	M	M	M	M
Daycare centers					
Evaluate whether to locate daycare facilities in buildings with high threat activities	N/A	M	M	M	M
Compare feasibility of locating daycare in facilities outside locations	N/A	M	M	M	M

Legend:
Minimum standard = M
Standard based on facility evaluation = F
Desirable = D
Not applicable = N/A

Source: Vulnerability Assessment of Federal Facilities, Department of Justice, June 28, 1995.

Table 4: Recommended Minimum Security Standards--Security Planning

SECURITY PLANNING	Facility Security Level				
	I	II	III	IV	V
Intelligence Sharing					
Establish law enforcement agency/security liaisons	M	M	M	M	M
Review/establish procedure for intelligence receipt and dissemination	M	M	M	M	M
Establish uniform security/threat nomenclature	M	M	M	M	M
Training					
Conduct annual security awareness training	M	M	M	M	M
Establish standardized unarmed guard qualifications/ training requirements	M	M	M	M	M
Establish standardized armed guard qualifications/ training requirements	M	M	M	M	M
Tenant Assignment					
Co-locate agencies with similar security needs	D	D	D	D	D
Do not co-locate high/low risk agencies	D	D	D	D	D
Administrative Procedures					
Establish flexible work schedule in high threat/high risk areas to minimize employee vulnerability to criminal activity	F	F	D	D	D
Arrange for employee parking in/near building after normal work hours	F	F	F	F	F
Conduct background security checks and/or establish security control procedures for service contract personnel	M	M	M	M	M
Construction/Renovation					
Install Mylar film on all exterior windows (shatter protection)	D	D	F	M	M
Review current projects for blast standards	M	M	M	M	M
Review/establish uniform standards for construction	M	M	M	M	M
Review/establish new design standards for blast Resistance	F	F	M	M	M
Establish street setback for new construction	D	D	F	M	M

Legend: Minimum standard = M
Standard based on facility evaluation = F
Desirable = D
Not applicable = N/A

Source: Vulnerability Assessment of Federal Facilities, Department of Justice, June 28, 1995.

DEPARTMENT OF COMMERCE

DOJ/DOC LEVEL (I) BUILDING

PHASED SECURITY ALERT GUIDELINES

ALERT LEVEL ONE
Low Condition (Green)

LOW
Low Risk of Terrorist Attacks

This condition is declared when a general threat of possible terrorist activity exists but warrants only a normal security posture. DOC operating units should consider the following general measures in addition to agency-specific protective measures that have been developed and implemented:

REQUIRED ACTIONS

- Refine and exercise preplanned protective measures, as appropriate.
- Ensure personnel receive proper training on the Homeland Security Advisory System and specific preplanned facility/agency protective measures.
- Institute a process to assure that all facilities are regularly assessed for vulnerabilities to terrorist attacks and all reasonable measures are taken to reduce these vulnerabilities.

ALERT LEVEL TWO
Guarded Condition (Blue)

GUARDED
General Risk of Terrorist

These actions are taken when there is a general threat of possible terrorist activity against customers, visitors, and facilities, the nature and extent of which are unpredictable and circumstances do not justify full implementation of Alert Level Three. The actions must be capable of being maintained indefinitely. In addition to the protective measures taken in the previous Alert Level, DOC operating units should implement additional and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level One.
- Check communications with designated emergency response or command locations.
- Review and update your continuity of operations plan (COOP) and emergency occupant plan (OEP) response procedures to include checking communications with designated emergency response personnel and agency phone trees.
- Provide your employees with any information that would strengthen their ability to act appropriately.

- At regular intervals, remind employees to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for suspicious vehicles on or adjacent to federal property. Watch for abandoned parcels or suitcases and any unusual activity.
- Ensure the building managers or representatives with access to building plans and occupant emergency plans are available at all times.
- Review all plans and requirements related to the implementation of higher security alert levels.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Increase security spot checks of vehicles and persons entering federal property.
- Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.
- Require U.S. Government identification for employees and state driver's license or comparable valid identification for visitors.
- Inspect and search all packages, handbags, and other containers, except those carried by persons displaying U.S. Government credentials. **DENY ENTRANCE TO ALL PERSONS WHO REFUSE THIS INSPECTION.**
- Check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors, and windows.
- Secure buildings, rooms, and storage areas not in regular use.
- Consult with local authorities on the threat and mutual anti-terrorism measures.
- Review and coordinate security measures for high-risk personnel as appropriate.
- After normal duty hours, ensure exterior and parking area lighting is operating properly in order to discourage intruders.

ALERT LEVEL THREE
Elevated Condition (Yellow)

ELEVATED
Significant Risk of Terrorist Attacks

These actions are taken when an increased and more predictable threat of terrorist activity exists. These actions must be capable of being maintained for weeks without causing undue hardship, affecting the operations of our customers, and aggravating relations with local authorities. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level Two.
- Increase the surveillance of critical locations.

- Coordinate emergency plans as appropriate with nearby jurisdictions.
- Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures.
- Implement contingency and emergency response plans, as appropriate.
- Warn customers of any potential form of terrorist attack.
- Keep all personnel involved in implementing anti-terrorist contingency plans on call.
- Check plans for the implementation of the next alert level.
- At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings (those in regular use) for suspicious packages.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Move unchecked cars and objects (i.e. crates, trash containers, etc.) at least 100 feet from buildings. Use other measures when distance cannot be achieved.
- Direct personnel who handle mail and deliveries to examine incoming material (above the regular examination process) for letter or parcel bombs.
- To build confidence among staff, increase contacts with individuals responsible for activities such as child care centers and agencies with high amounts of personal threat reporting.
- Make customers aware of the general situation in order to stop rumors and prevent unnecessary alarm.
- Implement additional security measures for high-risk personnel as appropriate.
- Consult local authorities on threat and mutual anti-terrorism measures.
- After normal duty hours, require all employees and visitors to sign the building register upon entering and leaving the building.

ALERT LEVEL FOUR
High Condition (Orange)

HIGH
High Risk of Terrorist Attacks

These actions are taken when an incident occurs or intelligence is received indicating that some form of terrorist action against customers and facilities is likely. Implementation of measures in this alert level for more than a short period probably will create hardship, affect the operations of our customers, and significantly increase operating costs. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue or introduce all measures listed in Alert Level Three.
- Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; keep all security personnel on immediate recall.

- Take additional precautions at public events and consider alternative venues or even cancellation.
- Prepare to execute continuity of operations plan, such as moving to an alternate site or dispersing the workforce.
- Restrict threatened facility access to essential personnel only.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Limit facility access points to the absolute minimum.
- Protect all designated vulnerable points.
- Strictly enforce control of entry. Randomly search vehicles.
- Increase patrol tempo of security guards and police officers.
- Erect barriers and obstacles to control traffic flow.
- Consult with local authorities about closing public streets that might make facilities more vulnerable to attacks.
- Restrict outside vehicular parking to 300 feet from the facility. Use other measures where distance cannot be achieved.

ALERT LEVEL FIVE
Severe Condition (Red)

SEVERE
Severe Risk of Terrorist Attacks

These actions are taken in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally this alert level is declared as a localized condition. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all actions listed in Alert Level Four.
- Assign emergency response personnel and preposition and mobilize specially trained teams or resources.
- Monitor, redirect, or constrain transportation systems.
- Increase or redirect personnel to address critical emergency needs.
- As directed by authorized officials, close the facility.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Control access and implement positive identification of all individuals with **NO EXCEPTIONS.**
- Thoroughly search all suitcases, briefcases, and packages brought into the building.
- Augment security guards as necessary.
- Search all vehicles and their contents before allowing entrance to the building.
- Make frequent checks of the exterior of the buildings and parking areas.
- Coordinate the possible closing of public streets and facilities with local authorities.
- Activate the facility OEP.

DEPARTMENT OF COMMERCE

DOJ/DOC LEVEL (II) BUILDING

PHASED SECURITY ALERT GUIDELINES

ALERT LEVEL ONE
Low Condition (Green)

LOW
Low Risk of Terrorist Attacks

This condition is declared when a general threat of possible terrorist activity exists but warrants only a normal security posture. DOC operating units should consider the following general measures in addition to the agency-specific protective measures that have been developed and implemented:

REQUIRED ACTIONS

- Refine and exercise preplanned protective measures, as appropriate.
- Ensure personnel receive proper training on the Homeland Security Advisory System and specific preplanned facility/agency protective measures.
- Institute a process to assure that all facilities are regularly assessed for vulnerabilities to terrorist attacks and all reasonable measures are taken to reduce these vulnerabilities.

ALERT LEVEL TWO
Guarded Condition (Blue)

GUARDED
General Risk of Terrorist

These actions are taken when there is a general threat of possible terrorist activity against customers, visitors, and facilities, the nature and extent of which are unpredictable and circumstances do not justify full implementation of Alert Level Three. The actions must be capable of being maintained indefinitely. In addition to the protective measures taken in the previous Alert Level, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level One.
- Check communications with designated emergency response or command locations.
- Review and update your continuity of operations plan (COOP) and emergency occupant plan (OEP) response procedures to include checking communications with designated emergency response personnel and agency phone trees.
- Provide your employees with any information that would strengthen their ability to act appropriately.

- At regular intervals, remind employees to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for suspicious vehicles on or adjacent to federal property. Watch for abandoned parcels or suitcases and any unusual activity.
- Ensure the building managers or representatives with access to building plans and occupant emergency plans are available at all times.
- Review all plans and requirements related to the implementation of higher security alert levels.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Increase security spot checks of vehicles and persons entering federal property.
- Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.
- Require U.S. Government identification for employees and state driver's license or comparable valid identification for visitors.
- Inspect and search all packages, handbags, and other containers, except those carried by persons displaying U.S. Government credentials. **DENY ENTRANCE TO ALL PERSONS WHO REFUSE THIS INSPECTION.**
- Check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors, and windows.
- Secure buildings, rooms, and storage areas not in regular use.
- Consult with local authorities on the threat and mutual anti-terrorism measures.
- Review and coordinate security measures for high-risk personnel as appropriate.
- After normal duty hours, ensure exterior and parking area lighting is operating properly in order to discourage intruders.

ALERT LEVEL THREE
Elevated Condition (Yellow)

ELEVATED
Significant Risk of Terrorist Attacks

These actions are taken when an increased and more predictable threat of terrorist activity exists. These actions must be capable of being maintained for weeks without causing undue hardship, affecting the operations of our customers, and aggravating relations with local authorities. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level Two.
- Increase the surveillance of critical locations.

- Coordinate emergency plans as appropriate with nearby jurisdictions.
- Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures.
- Implement contingency and emergency response plans, as appropriate.
- Warn customers of any potential form of terrorist attack.
- Keep all personnel involved in implementing anti-terrorist contingency plans on call.
- Check plans for the implementation of the next alert level.
- At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings (those in regular use) for suspicious packages.
- To build confidence among staff, increase contacts with individuals responsible for activities such as child care centers and agencies with high amounts of personal threat reporting.
- Make customers aware of the general situation in order to stop rumors and prevent unnecessary alarm.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Move unchecked cars and objects (i.e. crates, trash containers, etc.) at least 100 feet from buildings. Use other measures when distance cannot be achieved.
- Direct personnel who handle mail and deliveries to examine incoming material (above the regular examination process) for letter or parcel bombs.
- Implement additional security measures for high-risk personnel as appropriate.
- Consult local authorities on threat and mutual anti-terrorism measures.
- After normal duty hours, require all employees and visitors to sign the building register upon entering and leaving the building.

ALERT LEVEL FOUR
High Condition (Orange)

HIGH
High Risk of Terrorist Attacks

These actions are taken when an incident occurs, or intelligence is received indicating that some form of terrorist action against customers and facilities is likely. Implementation of measures in this alert level for more than a short period probably will create hardship, affect the operations of our customers, and significantly increase operating costs. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue or introduce all measures listed in Alert Level Three.
- Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; keep all security personnel on immediate recall.

- Take additional precautions at public events and consider alternative venues or even cancellation.
- Prepare to execute continuity of operations plan, such as moving to an alternate site or dispersing the workforce.
- Restrict threatened facility access to essential personnel only.
- Limit access points to the absolute minimum.
- Protect all designated vulnerable points.
- Limit facility access points to the absolute minimum.
- Protect all designated vulnerable points.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Strictly enforce control of entry. Randomly search vehicles.
- Increase patrol tempo of security guards and police officers.
- Erect barriers and obstacles to control traffic flow.
- Consult with local authorities about closing public streets that might make facilities more vulnerable to attacks.
- Restrict outside vehicular parking to 300 feet from the facility. Use other measures where distance cannot be achieved.

ALERT LEVEL FIVE
Severe Condition (Red)

SEVERE
Severe Risk of Terrorist Attacks

These actions are taken in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally this alert level is declared as a localized condition. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all actions listed in Alert Level Four.
- Assign emergency response personnel and preposition and mobilize specially trained teams or resources.
- Monitor, redirect, or constrain transportation systems.
- Increase or redirect personnel to address critical emergency needs.
- Control access and implement positive identification of all individuals with **NO EXCEPTIONS**.
- Thoroughly search all suitcases, briefcases, and packages brought into the building.

- Augment security guards as necessary.
- Search all vehicles and their contents before allowing entrance to the building.
- As directed by authorized officials, close the facility.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Make frequent checks of the exterior of the buildings and parking areas.
- Coordinate the possible closing of public streets and facilities with local authorities.
- Activate the facility OEP.
- Consider closing the facility.

DEPARTMENT OF COMMERCE

DOJ/DOC LEVEL (III) BUILDING

PHASED SECURITY ALERT GUIDELINES

ALERT LEVEL ONE
Low Condition (Green)

LOW
Low Risk of Terrorist Attacks

This condition is declared when a general threat of possible terrorist activity exists but warrants only a normal security posture. DOC operating units should consider the following general measures in addition to the agency-specific protective measures that have been developed and implemented:

REQUIRED ACTIONS

- Refine and exercise preplanned protective measures, as appropriate.
- Ensure personnel receive proper training on the Homeland Security Advisory System and specific preplanned facility/agency protective measures.
- Institute a process to assure that all facilities are regularly assessed for vulnerabilities to terrorist attacks and all reasonable measures are taken to reduce these vulnerabilities.

ALERT LEVEL TWO
Guarded Condition (Blue)

GUARDED
General Risk of Terrorist

These actions are taken when there is a general threat of possible terrorist activity against customers, visitors, and facilities, the nature and extent of which are unpredictable and circumstances do not justify full implementation of Alert Level Three. The actions must be capable of being maintained indefinitely. In addition to the protective measures taken in the previous Alert Level, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level One.
- Check communications with designated emergency response or command locations.
- Review and update your continuity of operations plan (COOP) and emergency occupant plan (OEP) response procedures to include checking communications with designated emergency response personnel and agency phone trees.
- Provide your employees with any information that would strengthen their ability to act appropriately.
- Require U.S. Government identification for employees and state driver's license or comparable valid identification for visitors.
- Inspect and search all packages, handbags, and other containers, except those carried by persons displaying U.S. Government credentials. **DENY ENTRANCE TO ALL PERSONS WHO REFUSE THIS INSPECTION.**

- At regular intervals, remind employees to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for suspicious vehicles on or adjacent to federal property. Watch for abandoned parcels or suitcases and any unusual activity.
- Ensure the building managers or representatives with access to building plans and occupant emergency plans are available at all times.
- Secure buildings, rooms, and storage areas not in regular use.
- Review all plans and requirements related to the implementation of higher security alert levels.
- Review and coordinate security measures for high-risk personnel as appropriate.
- Increase security spot checks of vehicles and persons entering property.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.
- Check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors, and windows.
- Consult with local authorities on the threat and mutual anti-terrorism measures.
- After normal duty hours, ensure exterior and parking area lighting is operating properly in order to discourage intruders.

ALERT LEVEL THREE
Elevated Condition (Yellow)

ELEVATED
Significant Risk of Terrorist Attacks

These actions are taken when an increased and more predictable threat of terrorist activity exists. These actions must be capable of being maintained for weeks without causing undue hardship, affecting the operations of our customers, and aggravating relations with local authorities. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level Two.
- Increase the surveillance of critical locations.
- Coordinate emergency plans as appropriate with nearby jurisdictions.
- Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures.
- Implement contingency and emergency response plans, as appropriate.
- Warn customers of any potential form of terrorist attack.
- Direct personnel who handle mail and deliveries to examine incoming material (above the regular examination process) for letter or parcel bombs.
- At early stages, inform the Building Security Committees of actions to be taken. Explain the reasons for the actions.
- Keep all personnel involved in implementing anti-terrorist contingency plans on call.
- Check plans for the implementation of the next alert level.

- At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings (those in regular use) for suspicious packages.
- To build confidence among staff, increase contacts with individuals responsible for activities such as child care centers and agencies with high amounts of personal threat reporting.
- Make customers aware of the general situation in order to stop rumors and prevent unnecessary alarm.
- After normal duty hours, require all employees and visitors to sign the building register upon entering and leaving the building.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Move unchecked cars and objects (i.e. crates, trash containers, etc.) at least 100 feet from buildings. Use other measures when distance cannot be achieved.
- Implement additional security measures for high-risk personnel as appropriate.
- Consult local authorities on threat and mutual anti-terrorism measures.

ALERT LEVEL FOUR
High Condition (Orange)

HIGH
High Risk of Terrorist Attacks

These actions are taken when an incident occurs, or intelligence is received indicating that some form of terrorist action against customers and facilities is likely. Implementation of measures in this alert level for more than a short period probably will create hardship, affect the operations of our customers, and significantly increase operating costs. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue or introduce all measures listed in Alert Level Three.
- Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; keep all security personnel on immediate recall.
- Take additional precautions at public events and consider alternative venues or even cancellation.
- Prepare to execute continuity of operations plan, such as moving to an alternate site or dispersing the workforce.
- Restrict threatened facility access to essential personnel only.
- Limit access points to the absolute minimum.
- Strictly enforce control of entry. Randomly search vehicles.
- Increase patrol tempo of security guards and police officers.
- Protect all designated vulnerable points.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Erect barriers and obstacles to control traffic flow.
- Consult with local authorities about closing public streets that might make facilities more vulnerable to attacks.
- Restrict outside vehicular parking to 300 feet from the facility. Use other measures where distance cannot be achieved.

ALERT LEVEL FIVE
Severe Condition (Red)

SEVERE
Severe Risk of Terrorist Attacks

These actions are taken in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally this alert level is declared as a localized condition. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all actions listed in Alert Level Four.
- Assign emergency response personnel and preposition and mobilize specially trained teams or resources.
- Monitor, redirect, or constrain transportation systems.
- Increase or redirect personnel to address critical emergency needs.
- Control access and implement positive identification of all individuals with **NO EXCEPTIONS**.
- Thoroughly search all suitcases, briefcases, and packages brought into the building.
- Augment security guards as necessary.
- Search all vehicles and their contents before allowing entrance to the building.
- As directed by authorized officials, close the facility.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Make frequent checks of the exterior of the buildings and parking areas.
- Coordinate the possible closing of public streets and facilities with local authorities.
- Activate the facility OEP.

DEPARTMENT OF COMMERCE

DOJ/DOC LEVEL (IV) BUILDINGS

PHASED SECURITY ALERT GUIDELINES

ALERT LEVEL ONE
Low Condition (Green)

LOW
Low Risk of Terrorist Attacks

This condition is declared when a general threat of possible terrorist activity exists but warrants only a normal security posture. DOC operating units should consider the following general measures in addition to the agency-specific protective measures you have developed and implemented:

REQUIRED ACTIONS

- Refine and exercise preplanned protective measures, as appropriate.
- Ensure personnel receive proper training on the Homeland Security Advisory System and specific preplanned facility/agency protective measures.
- Institute a process to assure that all facilities are regularly assessed for vulnerabilities to terrorist attacks and all reasonable measures are taken to reduce these vulnerabilities.

ALERT LEVEL TWO
Guarded Condition (Blue)

GUARDED
General Risk of Terrorist

These actions are taken when there is a general threat of possible terrorist activity against customers, visitors, and facilities, the nature and extent of which are unpredictable and circumstances do not justify full implementation of Alert Level Three. The actions must be capable of being maintained indefinitely. In addition to the protective measures taken in the previous Alert Level, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level One.
- Check communications with designated emergency response or command locations.
- Review and update your continuity of operations plan (COOP) and emergency occupant plan (OEP) response procedures to include checking communications with designated emergency response personnel and agency phone trees.
- Provide your employees with any information that would strengthen their ability to act appropriately.
- At regular intervals, remind employees to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for suspicious vehicles on or adjacent to federal property. Watch for abandoned parcels or suitcases and any unusual activity.
- Require U.S. Government identification for employees and state driver's license or comparable valid identification for visitors.

- Inspect and search all packages, handbags, and other containers, except those carried by persons displaying U.S. Government credentials. **DENY ENTRANCE TO ALL PERSONS WHO REFUSE THIS INSPECTION.**
- Ensure the building managers or representatives with access to building plans and occupant emergency plans are available at all times.
- Secure buildings, rooms, and storage areas not in regular use.
- Review all plans and requirements related to the implementation of higher security alert levels.
- Review and coordinate security measures for high-risk personnel as appropriate.
- Increase security spot checks of vehicles and persons entering property.
- Check basement, engineering spaces, heating and air conditioning ducts, shrubbery, and potential entry points such as roof openings, steam and other utility tunnels, doors, and windows.
- Review all plans and requirements related to the introduction of higher security alert levels.
- After normal duty hours, ensure exterior and parking area lighting is operating properly in order to discourage intruders.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.
- Consult with local authorities on the threat and mutual anti-terrorism measures.

ALERT LEVEL THREE
Elevated Condition (Yellow)

ELEVATED
Significant Risk of Terrorist Attacks

These actions are taken when an increased and more predictable threat of terrorist activity exists. These actions must be capable of being maintained for weeks without causing undue hardship, affecting the operations of our customers, and aggravating relations with local authorities. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all measures listed in Alert Level Two.
- Increase the surveillance of critical locations.
- Coordinate emergency plans as appropriate with nearby jurisdictions.
- Assess whether the precise characteristics of the threat require the further refinement of preplanned protective measures.
- Implement contingency and emergency response plans, as appropriate.
- Warn customers of any potential form of terrorist attack.
- Direct personnel who handle mail and deliveries to examine incoming material (above the regular examination process) for letter or parcel bombs.
- At early stages, inform the Building Security Committees of actions to be taken. Explain the reasons for the actions.

- Keep all personnel involved in implementing anti-terrorist contingency plans on call.
- Check plans for the implementation of the next alert level.
- At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings (those in regular use) for suspicious packages.
- To build confidence among staff, increase contacts with individuals responsible for activities such as child care centers and agencies with high amounts of personal threat reporting.
- Make customers aware of the general situation in order to stop rumors and prevent unnecessary alarm.
- After normal duty hours, require all employees and visitors to sign the building register upon entering and leaving the building.
- Move unchecked cars and objects (i.e. crates, trash containers, etc.) at least 100 feet from buildings. Use other measures when distance cannot be achieved.
- Implement additional security measures for high-risk personnel as appropriate.
- After normal duty hours, require all employees and visitors to sign the building register upon entering and leaving the building.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Consult local authorities on threat and mutual anti-terrorism measures.

ALERT LEVEL FOUR
High Condition (Orange)

HIGH
High Risk of Terrorist Attacks

These actions are taken when an incident occurs, or intelligence is received indicating that some form of terrorist action against customers and facilities is likely. Implementation of measures in this alert level for more than a short period probably will create hardship, affect the operations of our customers, and significantly increase operating costs. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the protective measures taken in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue or introduce all measures listed in Alert Level Three.
- Coordinate necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations; keep all security personnel on immediate recall.
- Take additional precautions at public events and consider alternative venues or even cancellation.
- Prepare to execute continuity of operations plan, such as moving to an alternate site or dispersing the workforce.
- Restrict threatened facility access to essential personnel only.

- Limit access points to the absolute minimum.
- Strictly enforce control of entry. Randomly search vehicles.
- Increase patrol tempo of security guards and police officers.
- Protect all designated vulnerable points.
- Erect barriers and obstacles to control traffic flow.
- Consult with local authorities about closing public streets that might make facilities more vulnerable to attacks.
- Restrict outside vehicular parking to 300 feet from the facility. Use other measures where distance cannot be achieved.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- NONE

ALERT LEVEL FIVE
Severe Condition (Red)

SEVERE
Severe Risk of Terrorist Attacks

These actions are taken in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally this alert level is declared as a localized condition. A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in the previous Threat Conditions, DOC operating units should implement the following general measures and/or agency-specific protective measures as necessary:

REQUIRED ACTIONS

- Continue all actions listed in Alert Level Four.
- Assign emergency response personnel and preposition and mobilize specially trained teams or resources.
- Monitor, redirect, or constrain transportation systems.
- Increase or redirect personnel to address critical emergency needs.
- Control access and implement positive identification of all individuals with **NO EXCEPTIONS**.
- Thoroughly search all suitcases, briefcases, and packages brought into the building.
- Augment security guards as necessary.
- Search all vehicles and their contents before allowing entrance to the building.
- Make frequent checks of the exterior of the buildings and parking areas.
- Coordinate the possible closing of public streets and facilities with local authorities.
- As directed by authorized officials, close the facility.

ACTIONS TO BE IMPLEMENTED AS DEEMED APPROPRIATE BY AUTHORIZED PERSONNEL

(Based on the threat and personnel available)

- Activate the facility OEP.