

**PHYSICAL SECURITY HANDBOOK  
FOR  
HUD REGIONAL AND FIELD OFFICES**



**HUD HANDBOOK**

**September 2007**

# U.S. Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Foreword

This *Handbook* provides policy and guidance to managers, supervisors, and staff members on the measures to be taken to ensure the physical security of HUD Regional and Field Offices nationwide. It acknowledges the security levels and minimum security standards established for federal office buildings in the United States in a report issued by the Department of Justice, *Vulnerability Assessment of Federal Facilities*, dated June 28, 1995, as well as modifications to those standards specified in the Federal Interagency Security Committee Subcommittee Final Report, *Security Standards for Leased Space*, dated May 16, 2003.

This *Handbook* lists and describes the security responsibilities of designated HUD officials and HUD offices. It also provides guidelines for conducting security and vulnerability assessments, coordinating among specified offices and agencies, preparing Office Physical Security Plans and Occupant Emergency Plans, and ensuring funding for the physical security program at all levels of the Department. In addition, the *Handbook* outlines a program of security training, education, and awareness for field managers, supervisors, and employees.

The Office of Security and Emergency Planning (OSEP), in coordination with the Office of Administrative and Management Services (OAMS) and the Office of Field Administrative Resources (OFAR), is responsible for ensuring the correctness and currency of the provisions of this *Handbook*. Any questions or comments should be referred to the Director, Physical Security Division, OSEP, at (202) 708-2914.

---

Keith A. Nelson

Assistant Secretary for Administration

**Department of Housing and Urban Development**  
**Physical Security Handbook for HUD Regional and Field Offices**  
**Record of Changes**

**U.S. Department of Housing and Urban Development  
Physical Security Handbook for HUD Regional and Field Offices**

**Contents**

|                         |     |
|-------------------------|-----|
| Foreword .....          | i   |
| Record of Changes ..... | ii  |
| Contents .....          | iii |

**Chapter 1. Introduction**

|  |     |
|--|-----|
| 1.1 Purpose .....                              | 1-1 |
| 1.2 Applicability and Scope .....              | 1-1 |
| 1.3 Authorities .....                          | 1-1 |
| 1.4 References .....                           | 1-1 |
| 1.5 Definition of Physical Security .....      | 1-2 |
| 1.6 Potential Threats/Vulnerabilities .....    | 1-2 |
| 1.7 Federal Security Design Philosophy .....   | 1-3 |
| 1.8 HUD Physical Security Policy .....         | 1-4 |
| 1.9 HUD Physical Security Advisory Group ..... | 1-4 |

**Chapter 2. Physical Security Standards for HUD Field Activities**

|   |     |
|---|-----|
| 2.1 General .....   | 2-1 |
| 2.2 Federal Security Levels .....   | 2-1 |
| 2.2.1 Typical Level I Facility .....                                      | 2-1 |
| 2.2.2 Typical Level II Facility .....                                     | 2-2 |
| 2.2.3 Typical Level III Facility .....                                    | 2-2 |
| 2.2.4 Typical Level IV Facility .....                                     | 2-3 |
| 2.2.5 Typical Level V Facility .....                                      | 2-3 |
| 2.3 Recommended Minimum Security Standards for HUD Field Activities ..... | 2-4 |

**Chapter 3. Responsibilities**

|  |     |
|--|-----|
| 3.1 General .....  | 3-1 |
| 3.2 Assistant Secretary for Administration .....                       | 3-1 |
| 3.2.1 Office of Security and Emergency Planning .....                  | 3-1 |
| 3.3 Deputy Assistant Secretary for Budget and Management Support ..... | 3-3 |
| 3.3.1 Office of Administrative and Management Services .....           | 3-3 |
| 3.3.2 Office of Budget and Administrative Services .....               | 3-3 |

**Chapter 3. Responsibilities (continued)**

3.4 General Deputy Assistant Secretary for Administration..... 3-3  
    3.4.1 Office of Field Administrative Resources..... 3-3  
3.5 Assistant Deputy Secretary for Field Policy and Management..... 3-3  
    3.5.1 Regional Directors..... 3-4  
    3.5.2 Field Office Directors..... 3-4  
    3.5.3 Office Security Coordinators..... 3-4

**Chapter 4. Implementation Guidelines**

4.1 General..... 4-1  
4.2 Risk Management Process..... 4-1  
4.3 Facility Security Assessment..... 4-1  
    4.3.1 Security Assessment Concept..... 4-1  
    4.3.2 Security Assessment Process..... 4-2  
4.4 Office Physical Security Plan..... 4-2  
4.5 Occupant Emergency Program..... 4-6  
    4.5.1 Occupant Emergency Organization (OEO)..... 4-6  
    4.5.2 Occupant Emergency Plan (OEP)..... 4-7  
4.6 Coordination..... 4-7  
    4.6.1 Lead Tenant..... 4-7  
    4.6.2 General Services Administration..... 4-7  
    4.6.3 Federal Protective Service..... 4-7  
    4.6.4 Other..... 4-8  
4.7 Physical Security Status Tracking and Reporting..... 4-8  
    4.7.1 Physical Security Status Checklist..... 4-8  
    4.7.2 Physical Security Status Review..... 4-9  
    4.7.3 Physical Security Status Reporting..... 4-9  
4.8 Physical Security Budgeting and Funding..... 4-10  
4.9 Physical Security Status Reports Overview..... 4-10

**Chapter 5. Training, Education, and Awareness**

5.1 General..... 5-1  
5.2 Training Objectives..... 5-1  
5.3 New Employee Orientation..... 5-1

## Chapter 5. Training, Education, and Awareness (*continued*)

|                                       |     |
|---------------------------------------|-----|
| 5.4 Security Training.....            | 5-1 |
| 5.4.1 Functional Training.....        | 5-2 |
| 5.4.2 Specialized Training.....       | 5-3 |
| 5.4.3 Annual Update.....              | 5-3 |
| 5.4.4 Training Records.....           | 5-3 |
| 5.5 Tests, Drills, and Exercises..... | 5-3 |
| 5.6 Security Awareness.....           | 5-4 |

### Appendices

|            |  |
|------------|--|
| Appendix A | Security Standards for Leased Space          |
| Appendix B | HUD Office Physical Security Plan            |
| Appendix C | Occupant Emergency Program                   |
| Appendix D | Contract Security Force Standards            |
| Appendix E | Facility Physical Security Status Checklist  |
| Appendix F | Field Office Physical Security Status Report |
| Appendix G | Regional Physical Security Status Report     |
| Appendix H | Urgent Physical Security Issue Report        |
| Appendix I | Glossary of Acronyms and Terms               |

# U.S. Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Chapter 1 - Introduction

#### 1.1 Purpose

This *Handbook* delineates definitive policy and guidance for establishing and maintaining effective physical security at HUD's Regional and Field Offices.

#### 1.2 Applicability and Scope

The provisions of this *Handbook* are applicable to all supervisors, managers, and staff members assigned to HUD Regional and Field Offices. The *Handbook* addresses: security standards for HUD field activities; roles and responsibilities; security and vulnerability assessments; preparation of Physical Security Plans and Occupant Emergency Plans (OEPs); security program budgeting and funding; and security training, education, and awareness.

#### 1.3 Authorities

- a. The National Security Act of 1947, dated July 26, 1947, as amended.
- b. Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended.
- c. Presidential Decision Directive 39, *U.S. Policy on Counterterrorism*, dated June 21, 1995.
- d. Executive Order 12977, *Interagency Security Committee*, dated October 19, 1995.
- e. Presidential Decision Directive 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, dated May 22, 1998.
- f. Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, dated December 17, 2003.
- g. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004.

#### 1.4 References

- a. Department of Justice, *Vulnerability Assessment of Federal Facilities*, dated June 28, 1995.
- b. Interagency Security Committee (ISC), *Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, dated May 28, 2001.
- c. U. S. General Accounting Office (GAO), *Key Elements of a Risk Management Approach*, dated October 12, 2001. (Note: Effective July 7, 2004, the GAO was renamed the Government Accountability Office.)
- d. General Services Administration, *Occupant Emergency Program Guide*, dated March 2002.

- e. HUD Deputy Secretary Memorandum, *Operating Protocols*, dated September 13, 2002.
- f. U. S. General Accounting Office, *Security Responsibilities for Federally Owned and Leased Facilities*, dated October 2002. (Note: Effective July 7, 2004, the GAO was renamed the Government Accountability Office.)
- g. Inter-Sec Group, *Report on Vulnerability Assessment of 25 Designated HUD Facilities*, dated January 22, 2003.
- h. ISC Subcommittee Final Report, *Security Standards for Leased Space*, dated May 16, 2003.
- i. Update of ISC, *Security Design Criteria for New Federal Office Buildings and Major Modernization Projects*, dated September 29, 2004.

### **1.5 Definition of Physical Security**

For the purposes of this *Handbook*, physical security is defined as that part of security concerned with physical measures to:

- Provide for the individual and collective safety and well-being of personnel, as well as visitors and clients;
- Prevent unauthorized access to a designated facility; and
- Protect and safeguard information, equipment, materials, and documents within the facility against espionage, sabotage, damage, theft, and/or unauthorized disclosure.

### **1.6 Potential Threats/Vulnerabilities**

Shown in Figure 1-1 are descriptions of the potential threats/vulnerabilities that may be applicable to any federal facility, as well as an indication of the likelihood that a given threat/vulnerability may present a problem for HUD Regional or Field Offices.

It should be noted that, irrespective of the likelihood of each of the potential threats/vulnerabilities identified, the physical security program of a given HUD facility must address each of these threats/vulnerabilities to some extent—with due consideration given to risk, cost, adverse impact due to loss, and other factors.

**Figure 1-1. Potential Threats/Vulnerabilities**

| Potential Threat/Vulnerability     | Description  | Likelihood  |
|------------------------------------|--|---|
| Security breaches                  | Deficiencies, inadequate training, and/or the absence of effective plans and procedures relative to controlling access to the facility, installed equipment, files and records, and information systems. | Likely, but can be minimized through proper corrective actions. (e.g., implementation of a comprehensive Physical Security Plan and OEP). |
| Non-hostile disruption of services | Disruption of utilities or support services (e.g., electrical power, water supply, environmental controls) due to non-hostile acts of nature or equipment failures or breakdowns.                        | Depends on a number of variables (location, service providers, age or condition of equipment, etc.).                                      |
| Hostile attack                     | Hostile use of conventional weapons or chemical, biological, or radiological agents to incapacitate or severely injure occupants of the facility.  | Unlikely, but depends on location (some areas are more likely than others).   |
| Hostile intelligence               | Penetration or compromise of the facility’s mission, installed equipment, or supporting infrastructures by hostile elements.   | Unlikely, but depends on location (some areas are more likely than others).   |

**1.7 Federal Security Design Principles**

Establishing and implementing an effective physical security program for each HUD facility should be undertaken in accordance with security design principles (as delineated by the ISC in reference 1.4b), including:

- Addressing the need to save lives and prevent injury, as well as protect the facility and its functions and assets.
- Taking a flexible and reasonable approach to the reliability, safety, and security of the facility;
- Considering cost effectiveness, geographic location, and urban design principles;
- Acknowledging the acceptance of some risk; and
- Recognizing that the facility must connect with the public in a reasonably open and accessible manner.

For construction of new office building space, and as appropriate, for major modernizations, the principles delineated by the ISC in reference 1.4i should be applied. Regional and Field Office staff involved in the project development, design and construction on behalf of HUD should

work with the agency in charge of the project (typically the General Services Administration) to ensure that those principles are met with respect to HUD facilities.

### **1.8 HUD Physical Security Policy**

Each HUD Regional and Field Office supervisor, manager, and individual employee is responsible for ensuring the safety, protection, and security of all information, resources, and property over which he/she has knowledge and control, as well as providing for the safety and well being of all occupants of the office. This policy will be put into effect in accordance with the standards and procedures specified in this *Handbook*.

### **1.9 HUD Physical Security Advisory Group**

The HUD Physical Security Advisory Group (PSAG) provides a forum to review, coordinate, and make recommendations on the processes and procedures that ensure the physical security of each HUD Regional and Field Office. The PSAG is chaired by the Director, Physical Security Division, Office of Security and Emergency Planning (OSEP). Membership consists of another staff member from OSEP; the Director, Office of Administrative and Management Services (OAMS); the Director, Office of Field Administrative Resources (OFAR), one representative of from the Office of Field Policy and Management (FPM); one Regional Office; and two Field Offices (one of which is located in a federal building and the other in leased space).

The PSAG may be involved in or assist with:

- a. Implementing a strategy for maintaining an effective physical security program for HUD Regional and Field Offices;
- b. Defining a multi-year physical security program budget;
- c. Complying with Presidential guidance and applicable criteria and standards for the physical security of HUD Regional and Field Offices;
- d. Providing information and recommendations within HUD for policy and planning for the physical security of Regional and Field Offices;
- e. Coordinating among OSEP, OAMS, OFAR, and FPM, on the resolution of physical security issues relative to HUD's Regional and Field Offices;
- f. Providing advice and assistance in ensuring that individual HUD Regional and Field Office Physical Security Plans and OEPs comply with prescribed criteria and standards; and
- g. Implementing a Test, Training, and Exercise (TT&E) program to evaluate the effectiveness of Physical Security Plans, OEPs, and implementing procedures for each HUD Regional and Field Office.

Any requests for PSAG advice and assistance, or recommendations concerning its activities, should be referred to the Director, Physical Security Division, OSEP, 202-708-2914.

## Chapter 2 - Physical Security Standards for HUD Field Activities

### 2.1 General

This Chapter presents the minimum physical security standards for HUD Regional and Field Offices. These standards are based on guidelines presented in:

- Department of Justice (DOJ) Report, *Vulnerability Assessment of Federal Facilities*, dated June 28, 1995 (see reference 1.4a in Chapter 1); and
- Interagency Security Committee (ISC) Subcommittee Final Report, *Security Standards for Leased Space*, dated May 16, 2003 (see reference 1.4h in Chapter 1) (see summary in Appendix A).

### 2.2 Federal Security Levels

Physical security standards for federal facilities are determined by five Federal Security Levels, which are generally based on the number of employees, size of the facility, use of the facility, and the need for public access. These levels from lowest to highest were specified in the Department of Justice (DOJ) report as Level I, Level II, Level III, Level IV, and Level V.

Based on a security survey conducted by the DOJ working group, the physical characteristics of typical facilities for each of the security levels were summarized as shown below. In addition, based on the working group's findings, the DOJ report provided the recommended security features that should be provided at each level. Further details on Governmentwide recommendations for Federal facilities are available in the DOJ report (reference 1.4a).

#### 2.2.1 Typical Level I Facility

A typical Level I facility has 10 or fewer federal employees (2,500 or less square feet of office space) and was found to have security-related physical characteristics such as:

- The federal agency is a single tenant in a leased office;
- The building has no set-back from the surrounding streets;
- There are other offices or business establishments in the building;
- There is metered and/or public parking immediately adjacent to the building;
- It is usually a satellite or small field office;
- The standard hours of operation are less than 12 hours a day;
- The building may or may not have perimeter lighting;
- The building may have rudimentary back-up power for emergency lighting and fire detection systems; and
- The facility most likely has high-security locks on all exterior doors; these locks are probably the primary measure of security for this level facility.

**Recommended security features for a Level I facility (in addition to high-security locks if not present) include:**

- Employee security awareness training;
- Perimeter lighting, with street lighting acceptable, and emergency power back-up desirable;
- Emergency back-up power for interior lighting;
- Occupant Emergency Organization officials assigned and trained; and
- Background security checks conducted on contract service personnel.

**2.2.2 Typical Level II Facility**

A typical Level II facility, most likely a multi-tenant, federally-owned or leased building, has between 11 and 150 federal employees (2,500 to 80,000 square feet of office space) and was found to have security-related physical characteristics such as:

- The building is likely to be multi-story;
- The building is likely to be older; there are many historical buildings in this category;
- With the exception of a sidewalk, the building is likely to have no setback from the surrounding streets;
- Only exterior parking is available, and it is adjacent to the building;
- The building operates an average of 12 hours a day; and
- As in a Level I facility, the primary security measure is high-security locks on all exterior doors.

**Recommended security features for a Level II facility (in addition to those recommended for Level I) include:**

- Perimeter lighting other than street lighting (again, emergency back-up power is desirable); and
- A visitor control and/or screening system, such as identification badges or sign-in register

**2.2.3 Typical Level III Facility**

A typical Level III facility, a multi-story, federally owned or leased building with several federal tenant organizations and 151 to 450 federal employees (80,000 to 150,000 square feet of office space), was found to have security-related physical characteristics such as:

- The building was constructed less than 25 years ago;
- Although the building has a greater set-back than would be found at a Level I or II facility, it still has only a minimal set-back from surrounding streets;
- It is likely to have an exterior parking lot;
- The building is open to employees more than 12 hours per day.

- As for Levels I and II, the primary security measure is high-security locks on all exterior doors; and
- The building may also have a centrally monitored intrusion detection system (IDS).

**Recommended security features for a Level III facility (in addition to those recommended for Levels I and II) include:**

- As much control as possible over interior parking, where available;
- Parking areas adjacent to federal space should be controlled when feasible;
- Perimeter lighting (for federally controlled facilities, the perimeter should be attached to a back-up power system);
- Magnetometer or x-ray screening at public entrances, as determined by local facility evaluations; and
- A security force, the size and locations to be determined by local facility evaluation.

**2.2.4 Typical Level IV Facility**

A typical Level IV facility, a large multi-tenant, federally owned or leased building with more than 450 federal employees (more than 150,000 square feet of office space), was found to have security-related physical characteristics such as:

- The building may be set back from the surrounding streets;
- Some interior underground parking as well as exterior parking is available;
- The building is accessible to employees more than 12 hours a day, and may be open to employees 24 hours per day;
- Public access is limited to less than 12 hours a day; and
- The building may have security officers stationed at entrances.

**Recommended security features for a Level IV facility (in addition to those recommended for Levels I, II, and III) include:**

- Control adjacent parking as much as possible;
- Use 24-hour closed circuit television (CCTV) with monitoring and videotape recording of the building's perimeter and with signs publicizing the presence of this equipment;
- Require that agency photo identification cards be displayed at all times;
- Have shatter-resistant exterior glass, or glass treated with a substance to resist shattering; and
- Require x-ray screening of all mail and packages brought into the building.

**2.2.5 Typical Level V Facility**

A typical Level V facility is a building such as the Pentagon or Central Intelligence Agency (CIA) Headquarters that is engaged in missions or functions critical to national security. A Level V facility is similar at a Level IV facility in terms of number of employees and square

footage. (NOTE: There are no HUD Regional or Field Offices located in a facility categorized as Level V.)

The above descriptions may not apply exactly to each HUD field activity for a given level, but generally indicate the distinctions between the levels that exist. Each HUD Regional and Field Office should have been assigned a Federal Security Level based on a facility security assessment by the Federal Protective Service (FPS). If such is not the case, the Office Director should request through appropriate channels that the FPS be contacted to officially validate the Federal Security Level of the office at the earliest opportunity.

### 2.3 Recommended Minimum Security Standards for HUD Field Activities

The following pages present recommended security standards for HUD Regional and Field Offices for Federal Security Levels I through IV, based on an analysis of the standards specified by DOJ for federal facilities and those prescribed for leased space by the ISC. The standards are delineated in the following charts:

Figure 2-1. HUD Office Security Standards—Perimeter Security;

Figure 2-2. HUD Office Security Standards—Interior Security;

Figure 2-3. HUD Office Security Standards—Entry Security; and

Figure 2-4. HUD Office Security Standards—Security Planning and Coordination.

The key to the symbols used in the charts is:

- M** Minimum standard (i.e., **mandatory**);
- S** Standard based on facility evaluation (i.e., standard will be met as practicable, but may vary from the minimum standard based on the local situation and/or conditions);
- D** Desirable (i.e., should be considered to enhance the security of the office); and
- N/A** Not applicable.

The recommended minimum security standards developed by the Department of Justice for HUD field locations will be used to guide and coordinate security planning for perimeter, entry, common area, and workspace areas. Any waivers/variations to the standards will be handled in accordance with the 2002 (Deputy Secretary Jackson, *Operating Protocols*, September 13, 2002) and 2007 (Secretary Jackson, *Strengthening Field Management Through Enhancement of Delegations of Authority and Operating Protocols*, February 13, 2007) Memorandum Delegations of Authority Protocols, as amended. All waivers in this regard must be in writing fully describing the need and basis for a variation. Waivers require the concurrence of OFAR or the Assistant Secretary for Administration.

For those standards that address the physical layout of or ancillary equipment provided at the host facility, the standard must be specified when negotiating new leases for HUD office space. In the case of long-term existing leases, every effort should be made to come as close to meeting each such standard as is reasonably possible.

Justification for or an explanation of not meeting a given security standard at a given HUD office should be recorded and retained on file as part of the Field Office Physical Security Status Report prepared annually for each office (see Chapter 4, sub-section 4.7.1, and Appendix F).

**Figure 2-1. HUD Security Standards – Perimeter Security**

| <b>Standard</b>  | <b>Level I</b> | <b>Level II</b> | <b>Level III</b> | <b>Level IV</b> |
|--|----------------|-----------------|------------------|-----------------|
| <b><i>Parking</i></b>  |                |                 |                  |                 |
| Access to facility parking is limited to government or other designated personnel and vehicles, and to authorized visitors.                            | <b>D</b>       | <b>D</b>        | <b>S</b>         | <b>S</b>        |
| Access controls to adjacent parking areas are in place to minimize threats to the facility and employee exposure to criminal activity.                 | <b>D</b>       | <b>D</b>        | <b>S</b>         | <b>S</b>        |
| Signs are posted to alert the public to parking restrictions, and arrangements have been made for towing unauthorized vehicles.                        | <b>S</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| A system and procedures are in place for identifying authorized vehicles and corresponding parking spaces (e.g., placards, decals, card keys, etc.).   | <b>D</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| Adequate lighting is provided in parking areas to ensure the safety of employees and authorized visitors, and deter illegal or threatening activities. | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Closed circuit television (CCTV) monitoring</i></b>  |                |                 |                  |                 |
| Twenty-four hour CCTV surveillance cameras with time-lapse video recording are used for monitoring exterior areas.                                     | <b>S</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| Signs are posted advising of 24-hour video surveillance.   | <b>S</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| <b><i>Exterior Lighting</i></b>  |                |                 |                  |                 |
| Lighting with emergency back-up power is provided along the building exterior and at entrances and exits.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Windows</i></b>  |                |                 |                  |                 |
| Shatter-resistant material has been applied to all exterior windows.   | <b>N/A</b>     | <b>S</b>        | <b>S</b>         | <b>M</b>        |
| <b><i>Physical barriers</i></b>  |                |                 |                  |                 |
| Physical barriers (concrete and/or steel composition) are in place along the perimeter of the facility.  | <b>N/A</b>     | <b>D</b>        | <b>D</b>         | <b>S</b>        |
| Parking barriers are in place to prevent unauthorized vehicle access.  | <b>N/A</b>     | <b>D</b>        | <b>D</b>         | <b>S</b>        |

**M** Minimum standard (mandatory)      **S** Standard based on facility evaluation      **D** Desirable      **N/A** Not applicable

**Figure 2-2. HUD Security Standards – Entry Security**

| <b>Standard</b>  | <b>Level I</b> | <b>Level II</b> | <b>Level III</b> | <b>Level IV</b> |
|--|----------------|-----------------|------------------|-----------------|
| <b><i>Access Control</i></b>   |                |                 |                  |                 |
| Security officer is posted at entrance(s) to control building access and/or access to HUD office space.  | <b>N/A</b>     | <b>D</b>        | <b>S</b>         | <b>S</b>        |
| An Intrusion Detection System (IDS) with central monitoring capability is installed at the building exterior.  | <b>S</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| Entry control is accomplished through installation of an automatic locking/remote unlocking mechanism on the entrance door(s) to HUD office space.   | <b>M</b>       | <b>M</b>        | <b>S</b>         | <b>S</b>        |
| An internal IDS is installed within HUD office space to preclude unauthorized entry into specified sensitive areas.  | <b>D</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| Life safety standards per General Services Administration (GSA) design standards (e.g., fire detection, fire suppression systems, etc.) are installed and operable.                                  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Entrances/Exits</i></b>  |                |                 |                  |                 |
| X-ray equipment and magnetometers (or comparable detection equipment) are installed at public entrances to the facility.   | <b>N/A</b>     | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| All mail/packages hand-carried into the building are subject to screening by x-ray machines and/or visual inspection.  | <b>N/A</b>     | <b>D</b>        | <b>S</b>         | <b>M</b>        |
| Glass door(s) is installed at the main entrance to HUD office space that permits visibility from within the immediate area outside of the entrance.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| HUD office space has at least two ways of egress, a front door and a back door. Preferably, the doors will not be located near each other and will open out into different hallways.                 | <b>D</b>       | <b>S</b>        | <b>M</b>         | <b>M</b>        |
| All exterior entrances/exits have high security locks that meet GSA specifications.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Receiving/Shipping Areas</i></b>   |                |                 |                  |                 |
| Package entry and access to receiving/shipping areas are controlled.   | <b>D</b>       | <b>S</b>        | <b>S</b>         | <b>M</b>        |
| <b><i>Posting of Government Rules and Regulations</i></b>  |                |                 |                  |                 |
| Federal government rules and regulations are posted at the entrance(s) to HUD-occupied space relative to policies such as prohibiting the unauthorized possession of firearms and dangerous weapons. | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |

**M** Minimum standard (mandatory)      **S** Standard based on facility evaluation      **D** Desirable      **N/A** Not applicable

**Figure 2-3. HUD Security Standards – Interior Security**

| Standard  | Level I    | Level II | Level III | Level IV |
|---|------------|----------|-----------|----------|
| <b><i>Receptionist Areas/Duress Alarm</i></b>   |            |          |           |          |
| A receptionist area is established facing the main entrance to HUD office space.  | <b>S</b>   | <b>S</b> | <b>M</b>  | <b>M</b> |
| The receptionist area is clearly visible from the interior of the office.   | <b>S</b>   | <b>S</b> | <b>M</b>  | <b>M</b> |
| The receptionist area has a hidden duress alarm that can be unobtrusively activated by the receptionist or other employee.                                  | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| The duress alarm annunciates at a monitoring station that is continuously staffed.  | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| Access to interior office space from the receptionist area is controlled by installation of card access mechanisms or cipher locks on doors leading inside. | <b>S</b>   | <b>S</b> | <b>S</b>  | <b>S</b> |
| <b><i>Employee/Visitor Identification/Control</i></b>   |            |          |           |          |
| All employees are issued a photo ID, which must be displayed at all times while in the HUD office.  | <b>N/A</b> | <b>D</b> | <b>M</b>  | <b>M</b> |
| All visitors sign in and out with a receptionist or security officer.   | <b>D</b>   | <b>D</b> | <b>D</b>  | <b>M</b> |
| All visitors are screened and issued a visitor ID badge, which must be displayed at all times while in the HUD office.                                      | <b>N/A</b> | <b>D</b> | <b>S</b>  | <b>S</b> |
| All visitors are accompanied by an escort while in the HUD office.  | <b>D</b>   | <b>D</b> | <b>D</b>  | <b>D</b> |
| <b><i>Mail and Package Handling</i></b>   |            |          |           |          |
| The mail and package handling and sorting area is isolated from other internal activities within the HUD office.  | <b>D</b>   | <b>S</b> | <b>M</b>  | <b>M</b> |
| Access to the mail and package handling area is restricted only to designated personnel.  | <b>D</b>   | <b>S</b> | <b>M</b>  | <b>M</b> |
| Personnel assigned to mail and package handling and sorting duties have been provided security training.  | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| Use of appropriate gloves is mandatory for all personnel handling incoming mail and packages.   | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| Procedures have been established for handling suspicious mail and packages, including provision of a repository for disposition of suspicious items.        | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| <b><i>Access to Sensitive Records and Equipment</i></b>   |            |          |           |          |
| The configuration and layout of the office precludes casual/unauthorized access to sensitive records.   | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| Access to computer workstations and printers, copiers, fax machines, etc., is restricted to authorized users.   | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |
| Access to telephone switching equipment is restricted to authorized users.  | <b>M</b>   | <b>M</b> | <b>M</b>  | <b>M</b> |

**M** Minimum standard (mandatory)      **S** Standard based on facility evaluation      **D** Desirable      **N/A** Not applicable

**Figure 2-3. HUD Security Standards – Interior Security (continued)**

| <b>Standard</b>  | <b>Level I</b> | <b>Level II</b> | <b>Level III</b> | <b>Level IV</b> |
|--|----------------|-----------------|------------------|-----------------|
| <b><i>Public Address System</i></b>  |                |                 |                  |                 |
| A public address system has been installed to permit emergency announcements to all occupants of HUD office space and/or the building in which the HUD office is located.  | <b>N/A</b>     | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| <b><i>Access to Public Restrooms</i></b>   |                |                 |                  |                 |
| Provisions have been made to restrict access to public restrooms to authorized personnel only.   | <b>N/A</b>     | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| <b><i>Utilities</i></b>  |                |                 |                  |                 |
| Utility areas in the facility in which the HUD office is located are secure and only authorized personnel can gain entry.  | <b>D</b>       | <b>S</b>        | <b>M</b>         | <b>M</b>        |
| Emergency back-up power to critical systems (e.g., alarm systems, radio communications, computer facilities, etc.) is available.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| Emergency lighting is provided throughout HUD office space, including illuminated exit signs powered by the emergency lighting system.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| A fire detection and suppression (sprinkler) system is installed that provides 100 percent coverage of HUD office space. *****   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Protection from airborne chemical, biological, or radiological (CBR) attack</i></b>  |                |                 |                  |                 |
| Access to fresh air intakes, mechanical areas, and roof tops in the facility in which the HUD office is located is strictly controlled.  | <b>S</b>       | <b>S</b>        | <b>S</b>         | <b>S</b>        |
| Access to building heating, ventilation, and air conditioning (HVAC) systems information is restricted to authorized personnel only.   | <b>S</b>       | <b>S</b>        | <b>S</b>         | <b>M</b>        |
| Procedures are in place for notification of the building manager, security force desk, local emergency personnel, and/or other key personnel in the event that toxic airborne hazards are suspected or detected. | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |

\*\*\*\*\* - Desirable in leased space but will depend on local fire code standards.

**M** Minimum standard (mandatory)      **S** Standard based on facility evaluation      **D** Desirable      **N/A** Not applicable

**Figure 2-4. HUD Security Standards – Security Planning and Coordination**

| <b>Standard</b>   | <b>Level I</b> | <b>Level II</b> | <b>Level III</b> | <b>Level IV</b> |
|---|----------------|-----------------|------------------|-----------------|
| <b><i>Physical Security Plan</i></b>  |                |                 |                  |                 |
| A comprehensive Physical Security Plan for the HUD office exists and is kept current.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| Copies of the Physical Security Plan are made available to all office employees.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| Provisions of the Physical Security Plan are made known to all employees through a comprehensive security training, education, and awareness program.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Occupant Emergency Program</i></b>  |                |                 |                  |                 |
| An Occupant Emergency Organization (OEO) has been established and includes the participation of all tenants in the facility in which the HUD office is located.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| An OEP is in place, updated annually, and periodically tested.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| Copies of the OEP are made available to all office employees.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| A formal OEP test, training, and exercise program has been established.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Standardized Alert Levels and Threat Conditions</i></b>   |                |                 |                  |                 |
| Standardized alert levels and threat terminology have been established.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| Procedures are in place to disseminate alert level and threat information to all concerned in a timely manner.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| Provisions have been made to jointly upgrade alert levels and security procedures in the facility in which the HUD office is located during emergency situations such as terrorist attacks, natural disasters, and/or civil unrest. | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Security Training, Education, and Awareness</i></b>   |                |                 |                  |                 |
| Security training and awareness materials have been developed and distributed, as appropriate, to provide up-to-date information covering security practices, employee security awareness, personal safety during emergencies, etc. | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| A formal security-training program has been established, including a new employee orientation and an annual update for all HUD employees.   | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |
| <b><i>Background Security Checks for Contract Service Personnel</i></b>   |                |                 |                  |                 |
| Background security checks and security control procedures are required for all contract service personnel within the facility in which the HUD office is located.  | <b>M</b>       | <b>M</b>        | <b>M</b>         | <b>M</b>        |

**M** Minimum standard (mandatory)      **S** Standard based on facility evaluation      **D** Desirable      **N/A** Not applicable

## **Chapter 3 - Responsibilities**

### **3.1 General**

The Office of Field Administrative Resources (OFAR) will assist Regional and Field Office Directors in the development and implementation of a comprehensive physical security program for their respective offices that complies with the objectives of this handbook. OFAR will coordinate day-to-day operational support for the local physical security programs including the provision of appropriate office space, and equipment pursuant to applicable HUD, GSA and ISC security standards. OFAR will also provide and/or arrange training for the Regional and Field Security Coordinators to be selected by the Regional and Field Office Directors in accordance with this handbook

The Director, Physical Security Division, OSEP, relies on the guidance and assistance of the Physical Security Advisory Group (PSAG) (see Section 1.9, Chapter 1) in developing and distributing standards and policies governing HUD's physical security program in the field. Funding to implement various physical security needs is provided through OFAR based upon the recommendations of FPM and the RDs and FODs.

### **3.2 Assistant Secretary for Administration**

The ASA is responsible for ensuring that physical security standards are established for all HUD Regional and Field Offices and for providing oversight of the adequacy of field security plans to protect HUD personnel, assets, and functions. This responsibility is carried out through the joint efforts and coordination among OSEP, the PSAG, FPM, OAMS, the Office of Budget and Administrative Support (OBAS), the Office of Field Administrative Resources (OFAR), RDs, and FODs. OBAS, through OFAR, RDs, and FODs, provides funding for physical security services and equipment in the field.

#### **3.2.1 Office of Security and Emergency Planning**

Within OSEP, the Director, Physical Security Division, relies on PSAG guidance and advice in developing physical security standards and systems for the field and monitors (in coordination with FPM and OFAR) the effectiveness of their implementation. With respect to determining appropriate solutions to significant physical security issues in Regional or Field Offices, the Director, Physical Security Division, will provide recommendations on corrective measures that could be taken to address the problem. However, ultimate responsibility for a decision on such matters rests with the RD or FOD of the office in question. Thus, the RD or FOD, with additional input from FPM and OFAR, will make the final decision on how to proceed to resolve the issue.

Specifically, the Director, Physical Security Division, is responsible for:

- a. Ensuring that FPM through the Regional and Field Directors coordinate with OFAR, for the Federal Protective Service (FPS) to perform a Facility Security Assessment for each office. The Facility Security Assessment will provide a comprehensive, independent evaluation of the security status of each office (see Section 4.3 in Chapter 4);

- b. Chairing the PSAG, which has been established to assist OSEP in the development of a strategy and standards for maintaining an effective physical security program for HUD Regional and Field Offices;
- c. Coordinating with the PSAG in developing and promulgating physical security standards and procedures for all Regional and Field Offices based on the ISC report, *Security Standards for Leased Space* (see reference 1.4h in Chapter 1), and additional security enhancements established by HUD;
- d. Coordinating with FPM through the RDs, FODs, and OFAR to ensure that there is a designated Security Coordinator in each Regional and Field Office;
- e. Coordinating with the PSAG in providing OAMS and OFAR with HUD security standards that are to be included in GSA leases for new leased office space in the field. Follow up with OAMS and OFAR to ensure that such standards are included in new GSA leases negotiated for Regional and Field Offices;
- f. Coordinating with the PSAG, RDs, FODs and OFAR in developing and distributing to the Regional and Field Office Security Coordinators information concerning no-cost security measures that should be implemented immediately upon receipt. Such information includes:
  - (1) Mandating that agency photo identification cards be displayed at all times by employees and contractors;
  - (2) Implementing procedures regarding visitor access and escort within the office;
  - (3) Issuing policy to ensure that office doors to staff space are locked at all times;
  - (4) Issuing policy concerning handling of incoming mail and packages; and
  - (5) In consultation with the OAMS Documents Division, issuing policy concerning protection and destruction of private and sensitive files;
- g. Developing, with input from the PSAG and in accordance with GSA certification guidelines, minimum standards for private non-federal contract security force services;
- h. Ensuring that OFAR, in coordination with the RDs, and FODs, develop a multi-year physical security budget that reflects security equipment and services identified in the office's Physical Security Plan. The OFAR Director should prioritize items included in the physical security budget request, with input from FPM and RDs and FODs. The budget should be incorporated into the consolidated budget request submitted to Headquarters by OFAR;
- i. Establishing and distributing standards and criteria for OEPs all HUD offices in the field to ensure consistency. In coordination with FPM and OFAR, and the Regional and Field Office Coordinators, oversee field compliance with specified OEP requirements; and
- j. Developing a system for sharing lessons learned about problematic security practices, and exemplary security practices that illustrate highly effective or innovative ways to address security issues in Regional and Field Offices among Security Coordinators.

### **3.3 Deputy Assistant Secretary for Budget and Management Support**

The Deputy Assistant Secretary for Budget and Management Support (BMS) provides support to OFAR and FPM in preparing annual and multi-year budget submissions to cover the cost of physical security equipment and services in HUD facilities in Washington, DC, and in Regional and Field Offices.

#### **3.3.1 Office of Administrative and Management Services**

The OAMS Space Design Branch (SDB) is responsible for conveying to GSA the HUD physical security requirements that exceed the ISC leased space security standards (see reference 1.4h in Chapter 1). The SDB Branch Chief coordinates with GSA and OFAR to ensure that all proposed new Regional and Field Office leases include the additional HUD physical security standards.

#### **3.3.2 Office of Budget and Administrative Services**

OBAS provides funds to the Regional and Field Offices for meeting their physical security equipment and services needs. Funding is provided through OFAR to work with the RDs and FODs in prioritizing funding needs within individual offices and across the region.

### **3.4 General Deputy Assistant Secretary for Administration**

The General Deputy Assistant Secretary for Administration oversees the operations of OFAR, which provides services to HUD field activities in the areas of administrative support for facilities, equipment, and supplies. This includes management oversight of the operations of OFAR in fulfilling the Office's responsibilities for supporting the Regional and Field Offices relative to physical security.

#### **3.4.1 Director, Office of Field Administrative Resources**

The Director of the Office of Field Administrative Resources provides administrative support to the RDs and FODs within the respective field jurisdictions. OFAR is responsible for obtaining equipment and services required for the security of Regional and Field Offices. OFAR coordinates with the OAMS SDB and GSA to negotiate leases for office space that meet both the ISC leased space security standards and additional HUD physical security requirements. OFAR is responsible for assisting the RDs and FODs develop Regional and Field Office's Physical Security Plans and OEPs to determine compliance with Sections 4.4 and 4.5 of this *Handbook*, respectively and assisting in the coordination efforts of the Regional Coordinators.

### **3.5 Assistant Deputy Secretary for Field Policy and Management**

The Secretary and Deputy Secretary of HUD, through the Assistant Deputy Secretary for FPM, have delegated substantial Field Office management and operational authority to the RDs, who in turn may re-delegate this authority to the FODs. Included in this delegation is the management of the work environment and key operational and administrative functions for management, oversight and development of office security plans, evacuation plans, and emergency procedures. FPM monitors field compliance and performance of these functions with OSEP and OFAR.

### **3.5.1 Regional Directors**

Regional Directors (RDs) are responsible for ensuring the protection of HUD employees, visitors, and property in the Regional Office and in Field Offices in their jurisdiction. Specific responsibilities include:

- a. In consultation with OFAR, designating an individual to serve as the Regional Security Coordinator for the Regional Office. The Regional Security Coordinator should be a designated staff member in OFAR, when practicable, to ensure coordination and oversight of the program through Administration. In the absence of an OFAR staff person on site, the Regional Coordinator may be assigned to a member of the RD's staff or a Program staff in consultation with the OFAR Director.
- b. Likewise, ensuring that each FOD, in consultation with OFAR designates an individual to serve as the Security Coordinator for the Field Office. The Field Office Security Coordinator should be the on-site Administrative Officer (AO), if available. In the absence of an on-site AO, or a designated OFAR staff person, this position could be assigned to a member of the FOD's staff or a Program Area staff person;
- c. Ensuring that the Regional Office and all Field Offices have an OEP that meets the basic requirements outlined in Section 4.5 of this *Handbook*;
- d. Identifying and prioritizing required Regional and Field Office security equipment and services, and requesting funding from the OFAR budget allocation; and
- e. Directing all FODs to ensure that an independent HUD Facility Security Assessment is accomplished at least every five years, or whenever significant changes in the facility, or its surroundings, have occurred.

### **3.5.2 Field Office Directors**

FODs are responsible for ensuring the protection of HUD employees, visitors, and property in their respective offices. Specific responsibilities include:

- a. In consultation with the OFAR Director , designating an individual to serve as the Field Office Security Coordinator for the office;
- b. Ensuring that the Field Office has an OEP that meets the requirements outlined in Section 4.5 of this *Handbook*;
- c. Conducting staff training on the OEP and scheduling periodic tests of emergency evacuation and shelter-in-place procedures;
- d. Ensuring that the office has a Physical Security Plan that has been developed in coordination with OFAR and submitted through the Regional Security Coordinator and OSEP for approval; and
- e. Identifying and prioritizing required office security equipment and services, and, with the approval of the RD, request funding from the OFAR budget allocation.

### **3.5.3 Regional and Field Office Security Coordinators**

- a. Regional Security Coordinator responsibilities include:
  - (1) Developing and testing the OEP for the Regional Office in leased facilities where HUD is the lead tenant;

- (2) Coordinating with GSA, FPS, and the lead federal agency tenant in federal buildings, and building management officials and tenants in privately leased space, on developing and testing the OEP;
  - (3) Maintaining close communication with OSEP and OFAR on developing and implementing OEPs and Physical Security Plans and resolving physical security problems;
  - (4) Providing technical assistance to the Field Office Security Coordinators on issues related to the OEPs and Physical Security Plans;
  - (5) Reviewing Field Office OEPs and Physical Security Plans for compliance with prescribed standards, and of approved plans to the Director, Physical Security Division, OSEP and FPM;
  - (6) Coordinating the scheduling of an independent Facility Security Assessment of the Regional Office at least every five years or whenever significant changes in the facility, or its surroundings, have occurred;
  - (7) Developing a physical security briefing for all new employees and an ongoing security awareness program for all Regional Office employees; and
  - (8) Implementing a system to ensure that procedures are in place to ensure the safety and security of the office when employees are working after normal business hours and on weekends.
- b. Field Office Security Coordinator responsibilities include:
- (1) Developing and testing the Field Office OEP in those cases where HUD is the lead tenant in leased space;
  - (2) Coordinating with the Regional Security Coordinator, GSA, DHS, and lead federal agency tenant in federal buildings, and with building management officials and tenants in privately leased space, on developing and testing the OEP;
  - (3) Preparing the Field Office Physical Security Plan, and upon approval by the FOD, submitting it through the Regional Security Coordinator for final approval;
  - (4) Maintaining close communications with the Regional Security Coordinator for technical assistance and guidance on OEPs and Physical Security Plans and to resolve problems;
  - (5) Coordinating the scheduling and preparation of an independent Facility Security Assessment of the Field Office at least every five years or whenever significant changes in the facility, or its surroundings, have occurred;
  - (6) Developing a physical security briefing for all new employees and an ongoing security awareness program for all Field Office employees; and
  - (7) Implementing a system to ensure that procedures are in place to ensure the safety and security of the office when employees are working after normal business hours and on weekends.

## Chapter 4 - Implementation Guidelines

### 4.1 General

This Chapter provides guidelines for implementing an effective physical security program for each HUD Regional and Field Office.

### 4.2 Risk Management Process

Because of the vast differences in the types of facilities occupied by HUD field activities and the variety of risks associated with each of them, there is no single approach to security that will work ideally for all buildings. Thus, it would be prudent to adopt a **risk management process** that has been followed by the federal intelligence and defense communities for many years (as cited by the GAO in numerous reports to the Congress, including references 1.4c and 1.4f in Chapter 1). This process entails the five basic steps described below.

- Identify assets—what are we protecting?
- Determine the threat—who are the adversaries?
- Analyze the vulnerabilities—how are we vulnerable?
- Assess risk—what are our priorities?
- Apply countermeasures—what can we do?

In this regard, risk management is defined as a systematic and analytical process that considers the likelihood that a threat will endanger assets, individuals, or functions at a given location and identifies actions that will reduce the risk and mitigate the consequences of an incident intended to harm, disrupt, or destroy a facility and its occupants. An effective risk management approach includes the following three primary elements listed below.

- **Threat assessment** is a process that identifies and evaluates the impact of conditions or potential adversaries that may cause injury, illness, or death of personnel, damage to or loss of equipment or property, or mission degradation.
- **Vulnerability assessment** is a process that identifies systemic weaknesses or shortcomings that may be exploited by potential adversaries or others and suggests options to eliminate or mitigate those weaknesses or shortcomings.
- **Criticality assessment** is a process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or functions, the group of people at risk, and/or the overall significance of a given facility in which a HUD activity is located.

### 4.3 Facility Security Assessment

The first step and principal product associated with application of the risk management process is developing an independent Facility Security Assessment for each HUD Regional and Field Office.

#### 4.3.1 Security Assessment Concept

A Facility Security Assessment for each HUD Regional and Field Office will be prepared every five years, or whenever significant changes in the facility or its environs have occurred.

It is important that the Assessment is conducted by a qualified representative(s) of an independent office or agency that does not have direct responsibility for the physical security of the office to be surveyed. Candidate agencies for conducting the Assessment include FPS, GSA, or a reputable security/vulnerability assessment contractor.

The most recent Assessment of a given HUD Regional or Field Office will serve as an official record of the security posture of a given office and will provide justification for instituting and funding any security enhancements deemed necessary.

#### **4.3.2 Security Assessment Process**

The Office Security Coordinator will arrange for and coordinate the scheduling and conduct of the security survey on which the Assessment will be based. Coordination and scheduling will be accomplished with the OFAR, Regional Office (for Field Offices), OSEP, FPM, and others, as appropriate.

The proposed format and contents for recording the results of a HUD Office Security Assessment are illustrated in Figure 4-1. The introductory descriptive information and parts 1 through 9 of the Assessment form will be completed by the office or agency conducting the security survey. Part 10 will be completed by the applicable HUD Regional Security Coordinator and, upon approval by the RD, will present the official HUD affirmation of the Assessment and/or any exception(s) to or amplification of information contained therein.

Copies of the Assessment will be provided to FPM and OSEP in HUD Headquarters.

#### **4.4 Office Physical Security Plan**

Each HUD Regional and Field Office will have a current Physical Security Plan that delineates the procedures to be followed and systems and equipment to be employed to provide for the safety and well being of personnel, protect and safeguard information, equipment, and materials within the office, and preclude unauthorized access to the facility.

An outline of the organization and content of an Office Physical Security Plan is illustrated in Figure 4-2. More detailed information is presented in Appendix B.

**Figure 4-1 - HUD Facility Security Assessment**

|   |                |                 |             |
|---|----------------|-----------------|-------------|
| Security Assessment of _____ (Regional or Field Office)   |                |                 |             |
| Date: _____   |                |                 |             |
| Survey conducted by (Name): _____   |                |                 |             |
| Organization: _____   |                |                 |             |
| <b>Description:</b>   |                |                 |             |
| HUD Region: _____   |                |                 |             |
| Address: _____  |                |                 |             |
| Space Ownership: Leased___ Federal ___  |                |                 |             |
| Number of Employees: _____  |                |                 |             |
| Gross Square Footage of the HUD Facility: _____   |                |                 |             |
| Federal Security Level: _____ (see Chapter 2.2 for criteria of Level I, II, III, IV, V)   |                |                 |             |
| <b>Name, Phone Number and E-Mail Address of On-Site Office Security Coordinator:</b>  |                |                 |             |
| _____   |                |                 |             |
| _____   |                |                 |             |
| _____   |                |                 |             |
| <b>Threat Level:</b>  | Low ___        | Medium ___      | High ___    |
| <b>Risk Level:</b>  | Low ___        | Medium ___      | High ___    |
| <b>Comments:</b>  |                |                 |             |
| <b>Nature of Surrounding Area:</b>  |                |                 |             |
| Commercial ___  | Industrial ___ | Residential ___ | Other _____ |
| Urban ___   | Suburban ___   | Rural ___       |             |
| <b>Comments:</b>  |                |                 |             |
| <b>Type of Facility:</b> _____  |                |                 |             |
| <i>[Indicate whether office building, warehouse, storefront, commercial building, school building, etc.]</i>  |                |                 |             |
| <b>1. Perimeter Security</b>  |                |                 |             |
| <i>[Scope: Parking controls; signage; exterior lighting with back-up power; CCTV monitoring; physical barriers; setback distance; security patrols; shatter-resistant windows; etc.]</i>  |                |                 |             |
| <b>2. Entry Security</b>  |                |                 |             |
| <i>[Scope: Access control; number of entrances/exits; security officers; ID/pass control; mail and package handling; intrusion detection system; magnetometers; peep holes; intercom system; entry control CCTV; high security locks; etc.]</i>   |                |                 |             |
| <b>3. Interior Security</b>   |                |                 |             |
| <i>[Scope: Employee/visitor ID; access to utility areas; HVAC location, controls, and accessibility; intrusion detection system(s); emergency back-up power for critical systems; receptionist duress alarms; public address system; mail handling areas and procedures; threat monitoring; etc.]</i> |                |                 |             |

#### **4. Security Planning and Coordination**

*[Scope: Availability and currency of Office Physical Security Plan; availability and currency of the OEP, facility physical security force organization and qualifications; administrative policies/procedures; proximity to local law enforcement and fire and rescue activities; security training, education, and awareness program; etc.]*

**Figure 4-1 - HUD Facility Security Assessment (continued)**

|   |   |
|---|---|
| Security Assessment of _____<br>(Regional or Field Office)  | Date: _____<br>Survey conducted by (Name): _____<br>Organization: _____ |
| <b>5. Perceived Threats</b>   |   |
| <i>[Identification and evaluation of conditions or potential adversaries that may cause injuries to occupants, damage to equipment or property, or mission degradation.]</i>  |   |
| <b>6. Perceived Vulnerabilities</b>   |   |
| <i>[Identification of weaknesses or shortcomings that may adversely affect the ability of the office to accomplish its mission and ensure the safety and security of its employees and the public.]</i>                             |   |
| <b>7. Criticality Assessment</b>  |   |
| <i>[Assessment of the entire complex in which the office is located to determine its criticality as a potential target for hostile elements.]</i>   |   |
| <b>8. General Comments Not Covered Above</b>  |   |
| <i>[Any other information concerning the facility that may have an impact on the security of the HUD office.]</i>   |   |
| <b>9. Recommendations</b>   |   |
| <i>[Based on the above findings, validate the Federal Security Level for the facility. If a change is recommended, provide justification. Also, identify any security enhancements deemed necessary, including estimated cost.]</i> |   |
| <b>10. HUD Comments</b>   |   |
| <i>[Indicate agreement with the findings of the security assessment; or identify any exceptions, stating the reason(s) why.]</i>  |   |

**Figure 4-2. Outline – HUD Office Physical Security Plan**

|  |
|--|
| <p><b>PART 1. INTRODUCTION</b></p> <p><b>PART 2. PERTINENT INFORMATION</b></p> <p style="padding-left: 20px;">2.1 DESCRIPTION OF FACILITY</p> <p style="padding-left: 20px;">2.2 DESCRIPTION OF SURROUNDING AREA</p> <p style="padding-left: 20px;">2.3 PROXIMITY TO EMERGENCY SERVICES</p> <p style="padding-left: 20px;">2.4 FACILITY/OFFICE PHYSICAL SECURITY ORGANIZATION</p> <p style="padding-left: 20px;">2.5 KEY TELEPHONE NUMBERS</p> <p><b>PART 3. PERIMETER SECURITY</b></p> <p><b>PART 4. ENTRY SECURITY</b></p> <p><b>PART 5. INTERIOR SECURITY</b></p> <p><b>PART 6. COORDINATING INSTRUCTIONS</b></p> |
|--|

A brief summary of the contents of a HUD Office Physical Security Plan (Plan) is provided below.

- **Part 1, Introduction**, will describe the purpose of the Plan, plus applicability and scope, authorities, and security responsibilities of all occupants of the office.
- **Part 2, Pertinent Information**, will contain the pertinent security-related information concerning the facility and environs shown in Figure 4-2. In addition, this part of the Plan should also include the Federal Security Level of the facility, whether the facility is leased space or federally owned and other information such as office population and physical characteristics of the building.
- **Part 3, Perimeter Security**, will address security measures taken for the protection and safeguarding of personnel, vehicles, and equipment in the external areas of the facility in which the HUD office is located. This will include parking areas and controls, exterior lighting, surveillance systems, and security control posts and patrols.
- **Part 4, Entry Security**, will address security measures taken for the protection of occupants and imposition of controls relative to the entry of persons, equipment, mail, and packages into the building in which the HUD office is located and into the HUD office itself.
- **Part 5, Interior Security**, will address security measures taken for the protection and safeguarding of occupants, information, equipment, and materials within the building in which the HUD office is located and within the HUD office itself against espionage, sabotage, damage, theft, and/or unauthorized access.
- **Part 6, Coordinating Instructions**, of the Plan will address essential across-the-board relevant matters such as security-related administrative policies and procedures, communications/computer systems security, contingency readiness and reporting, coordination with other local federal agencies, and security education, training, and awareness.

HUD Regional and Field Offices should develop their individual Plans at the earliest opportunity in accordance with the guidance contained in this *Handbook*. To facilitate this process, the Physical Security Division, OSEP, has developed a HUD Office Physical Security Plan template that provides specific, detailed guidance and assistance for Plan development. You may request a copy of the template via e-mail at [physical\\_security\\_office@hud.gov](mailto:physical_security_office@hud.gov) or by calling OSEP on 202-708-2914.

## **4.5 Occupant Emergency Program**

All federal facilities must have an Occupant Emergency Program encompassing procedures for safeguarding and protecting lives and property in and around the facility during emergencies. Key elements of an Occupant Emergency Program are an Occupant Emergency Organization and an OEP. A description and details of such a program are presented in the GSA *Occupant Emergency Program Guide* (see reference 1.4d in Chapter 1).

### **4.5.1 Occupant Emergency Organization (OEO)**

An OEO consists of a group of employees who are responsible for carrying out the Occupant Emergency Program. In offices where there is an existing Health and Safety Committee, the

Office Director could designate this committee as the OEO, with additional members appointed as needed to perform specific OEO functions. In a multi-agency facility, the employees who make up the OEO are primarily selected from the lead tenant, with representation from other agencies added as necessary to ensure a unified approach to dealing with an emergency.

Details concerning the composition and responsibilities of an OEO are presented in Appendix D.

#### **4.5.2 Occupant Emergency Plan (OEP)**

An OEP is a set of procedures designed to protect life and property in federally-occupied space under defined emergency conditions. The emergency may include a fire, explosion, discovery of an explosive device, actual or potential exposure to hazardous substances, severe weather, a natural disaster, such as a hurricane or earthquake, chemical, biological, or radiological threat or exposure, workplace violence, hostage takeover, or physical threat to the building, occupants, or visitors. Details concerning the format and contents of an OEP are presented in Appendix D.

### **4.6 Coordination**

Regardless of the type or location of the HUD Regional or Field Office facility, it is imperative that there be coordination and cooperation among all of the tenants within the facility. This should include the sharing of information and resources, if need be, to ensure the safeguarding and protection of all of the occupants and assets located in the facility.

#### **4.6.1 Lead Tenant**

Based on security standards and guidance for federally-owned facilities (presented in reference 1.4a in Chapter 1), the lead (“largest”) tenant will maintain OEP responsibility. Per reference 1.4h, this is also true for leased space (which in this case is construed to mean the lead federal tenant). In the event that the HUD office within a given facility is the lead tenant, this means that the HUD office has the responsibility for preparation of the local OEP, staffing the OEO, and arranging for the participation of other tenants in the facility. In the case that the HUD office within a facility is not the lead tenant, action should be taken to establish close relations with the lead tenant to ensure the safety and well being of HUD employees in the event of an emergency situation requiring implementation of the local OEP.

#### **4.6.2 General Services Administration (GSA)**

GSA is responsible for administering programs to manage and operate government-owned and leased property. In this capacity, GSA executes leases for office and other space to be used by federal departments and agencies. Thus, it is essential that OFAR project management staff in coordination with the Regional and/or Field Office Director, work closely with GSA to ensure that physical security is adequately addressed in the space requirements package provided to GSA prior to negotiating and executing (or re-negotiating) a lease for space to be used by HUD activities. In addition, GSA should be contacted any time there is need for security enhancements in response to new or changing threat conditions.

#### **4.6.3 Federal Protective Service (FPS)**

FPS (formerly part of GSA, now part of the Department of Homeland Security) provides law enforcement and security services to tenants of federally owned and leased facilities nationwide. FPS provides security officers and other security support at some, but not all, facilities at which HUD field activities are located. FPS, where present, may assist in the development and implementation of local OEPs through activities such as:

- Providing advice and assistance concerning emergency planning and organization;
- Helping train employees and other personnel on workplace safety and security-related emergency procedures;
- Providing technical support to operate utilities, such as generators;
- Providing protective equipment and materials; and
- Chairing the Building Security Committee (if one has been established).

HUD Regional and Field Offices should avail themselves of FPS expertise and services in accordance with local or regional policies and agreements. OFAR may request or coordinate a request that FPS conduct a physical security survey of the office as part of the Facility Security Assessment process (see section 4.3 above).

#### **4.6.4 Other**

Liaison should be established with local emergency response organizations, such as law enforcement, and fire and rescue. Phone numbers should be prominently displayed and included in the local Physical Security Plan and OEP.

In Regional and Field Offices where there are outstationed Office of the Inspector General (OIG) personnel, the IG agents could be requested to assist in resolving any immediate threats to the safety or security of HUD employees or visitors during emergencies.

If a bona fide need exists, OFAR may contract directly with the private sector for security force support in a Regional or field office, provided that such security force personnel are fully trained and qualified based on the federal standards established by FPS for its security force personnel (see Appendix E, Contract Security Force Standards).

### **4.7 Physical Security Status Tracking and Reporting**

It is essential that an orderly process be established for the periodic determination of the security status of each HUD Regional and Field Office, as described in the following sub-sections.

#### **4.7.1 Physical Security Status Checklist**

Appendix F presents a Checklist that contains key security-related requirements that should be periodically reviewed and evaluated in each Regional and Field Office. This Checklist is an internal document to be filled in by Regional and Field Office Security Coordinators as a means for assessing the security posture of the respective HUD Regional or Field Offices vis-à-vis the minimum physical security standards specified for HUD field activities (presented in Chapter 2 of this *Handbook*). Information contained in a completed Checklist will serve to augment or update the independent Facility Security Assessment conducted on a five-year cycle (see Section 4.3 above).

This Checklist will be retained on file and updated annually. Specifically, information derived from the Checklist will provide input for preparation of the annual Regional and Field Office Physical Security Status Report, described in Sub-sections 4.7.3 a and b, respectively, below.

#### **4.7.2 Physical Security Status Review**

In addition, the physical security status of each Regional and Field Office will be reviewed on a regular basis by outside entities. This review may take place:

- a. As part of the scheduled Quality Management Review (QMR) of the office;
- b. During routine operational visits by OFAR personnel;
- c. During routine operational visits by FPM Desk Officers; or
- d. During unannounced visits by staff members from the Physical Security Division, OSEP, to designated Regional or Field Offices deemed to have potentially serious security threats or vulnerabilities.

Among other elements of office security that may be examined by the above entities, portions of the completed Physical Security Status Checklist retained on file in each office may be used as the basis for expediting follow-up action(s) relative to perceived problem areas or issues.

Regional and Field Office Security Coordinators are responsible for taking and/or coordinating appropriate corrective action(s) to address deficiencies identified during scheduled or unannounced security reviews.

#### **4.7.3 Physical Security Status Reporting**

Formal reporting of security status will be conducted as described below.

- a. Field Offices. Annually, each Field Office Director/Security Coordinator will submit to the Regional Director/Security Coordinator a *Field Office Physical Security Status Report* that: describes security problems and improvements; lists unmet security needs; and provides an overall assessment of the physical security status in the Field Office. Once reviewed and approved by the Field Office Director, each Field Office will submit the Report by October 15 of each year. For the format and content of this report, see Appendix G.
- b. Regions. Annually the Regional Director/Security Coordinator will prepare a *Regional Physical Security Status Report*. This Regional Report will include the security status of the Regional Office, plus copies of all Field Office reports. Once reviewed/approved by the Regional Director, the report will be submitted to the Director, Physical Security Division, OSEP, no later than October 31 of each year, with copies to the HUD Headquarters office of FPM. For the format and content of this report, see Appendix H.
- c. Urgent Physical Security Issues. Reports concerning urgent physical security issues in Regional or Field Offices requiring immediate attention should be submitted via e-mail at any time to the Regional Director/Security Coordinator (for Field Offices), the Director of OFAR, and FPM. The Regional Director/Security Coordinator and

FPM should forward their comments and/or recommendations along with the report to the Director, Physical Security Division, OSEP. For the format and content of such reports, see Appendix I.

#### **4.8 Physical Security Budgeting and Funding**

HUD's comprehensive physical security program for Regional and Field Offices will identify recommended enhancements needed to ensure a safe and secure workplace environment. The annual Physical Security Status Report to be developed for each office, as well as the periodic Facility Security Assessment (see Section 4.3 above), will provide detailed information on the various security measures, including priorities that are recommended to be implemented over a period of time. OFAR, in coordination with FPM, OSEP, RDs, and FODs, will develop a HUD Field Activities Physical Security Multi-Year Strategy and Program Management Plan that will include the prioritized funding needs for physical security in the respective RDs and FODs. Upon approval by the ASA, physical security budgetary line items for each Regional and Field Office will be incorporated into the field administration fiscal year budget.

#### **4.9 Physical Security Status Reports Overview**

An overview of the physical security status reporting process for HUD Regional and Field Offices is presented in Figure 4-3.

**Figure 4-3 - HUD Regional/Field Office Physical Security Status Reports Overview**

| Report or Document   | Purpose  | Prepared by   | Approved by   | Distribution   | Timeline   |
|--|--|---|---|--|--|
| <p><b>Facility Security Assessment</b><br/>(Section 4.3)</p>                                       | <p>Provides a comprehensive summary of the security status of a HUD Regional or Field Office in terms of measures that exist or are recommended to protect and safeguard personnel, information, and property commensurate with perceived threats and vulnerabilities.</p> <p>Will be retained on file as the baseline document reflecting the physical security status of the office, unless made obsolete by a subsequent assessment or physical security status report.</p>   | <p>An independent office or agency such as the FPS, GSA, or a reputable security/vulnerability assessment contractor.</p> | <p>Regional Director</p>  | <ul style="list-style-type: none"> <li>▪ OFAR</li> <li>▪ FPM</li> <li>▪ OSEP</li> </ul>  | <p>Will be conducted every five years, or whenever significant changes in the facility or its environs have occurred.</p>  |
| <p><b>Physical Security Status Checklist</b><br/>(Sub-section 4.7.1 and Appendix F)</p>            | <p>This is an internal document that provides a means for assessing the security posture of a HUD Regional or Field Office vis-à-vis the minimum physical security standards specified for HUD field activities (presented in Chapter 2 of this <i>Handbook</i>).</p> <p>Serves to augment or update the <i>Facility Security Assessment</i>. Provides input for preparation of the annual <i>Office Physical Security Status Report</i>.</p> <p>OFAR, FPM, or OSEP personnel may use portions of a completed checklist, or Headquarters QMR teams for expediting follow-up action(s) relative to perceived problem areas or issues.</p> | <p>Regional and/or Field Office Security Coordinator</p>  | <p>Regional/Field Office Director</p>                               | <p>Upon request, copies may be distributed to:</p> <ul style="list-style-type: none"> <li>▪ OFAR</li> <li>▪ FPM</li> <li>▪ OSEP</li> </ul>           | <p>Will be completed annually in preparation for completing and submitting the <i>Physical Security Status Report</i> for the office.</p> <p>See next two items below.</p>                         |
| <p><b>Field Office Physical Security Status Report</b><br/>(Sub-section 4.7.3a and Appendix G)</p> | <p>A two-part report that summarizes security-related training activities, etc., conducted during the year; describes security problems and actions taken; provides an overall assessment of the security posture of the office; and summarizes recommended corrective actions.</p> <p>Part I is the basic report prepared by the Field Office, and Part II presents Regional Office comments.</p>   | <p>Part I: Field Office Security Coordinator<br/>Part II: Regional Security Coordinator</p>                               | <p>Part I: Field Office Director<br/>Part II: Regional Director</p> | <p>Part I: By each Field Office to the appropriate Regional Office.<br/>Part II: See next item, <i>Regional Physical Security Status Report</i>.</p> | <p>Field Office reports (Part I) will be submitted to the appropriate Regional Office by October 15 of each year.<br/>Part II: See next item, <i>Regional Physical Security Status Report</i>.</p> |

**Figure 4-3. HUD Regional/Field Office Physical Security Status Reports Overview (continued)**

| Report or Document  | Purpose  | Prepared by  | Approved by                           | Distribution  | Timeline   |
|---|--|--|---------------------------------------|---|--|
| <p><b>Regional Physical Security Status Report</b><br/>(Sub-section 4.7.3b and Appendix H)</p>    | <p>A composite Regional report that summarizes highlights of region-wide areas of concern, security-related incidents, security issues, lessons learned, initiatives undertaken, overall security posture, recommendations, etc. Includes as enclosures: (1) a physical security status report on the Regional Office itself; and (2) copies of the individual <i>Field Office Physical Security Status Reports</i> with Part II, Regional Comments, of those reports completed by the region.</p> | Regional Security Coordinator                      | Regional Director                     | Submitted to Director, Physical Security Division, OSEP, with copies to FPM   | Completed and submitted by October 31 of each year.  |
| <p><b>Urgent Physical Security Issue Report</b><br/>(Sub-section 4.7.3c and Appendix I)</p>       | <p>Provides a means for a HUD Regional or Field Office to report to all concerned a physical security issue(s) that requires immediate attention.</p>  | Regional and/or Field Office Security Coordinator  | Regional and/or Field Office Director | <ul style="list-style-type: none"> <li>▪ Applicable Region (for a report submitted by a Field Office)</li> <li>▪ FPM</li> <li>▪ Director, Physical Security Division, OSEP</li> </ul>   | Submitted as soon as possible after an issue(s) is recognized.   |
| <p><b>Physical Security Multi-year Strategy and Program Management Plan</b><br/>(Section 4.8)</p> | <p>Provides a mechanism for incorporating and prioritizing recommended HUD Regional and Field Office physical security projects and enhancements into the overall HUD budgeting and funding process. Source data for compilation of this Plan are derived from each <i>Facility Security Assessment</i>, and <i>Regional and Field Office Physical Security Status Reports</i>.</p>  | OFAR in coordination with FPM, OSEP, RDs, and FODs | ASA                                   | <ul style="list-style-type: none"> <li>▪ Deputy Assistant Secretary for Operations</li> <li>▪ Assistant Deputy Secretary for FPM</li> <li>▪ Director, OBAS</li> <li>▪ Director, OSEP</li> <li>▪ Director, OFAR</li> <li>▪ Regional Directors</li> <li>▪ Field Office Directors</li> </ul> | Approved physical security budgetary line items are incorporated into the Field Administrative fiscal year budget. |

## **Chapter 5 - Security Training, Education, and Awareness**

### **5.1 General**

All occupants of HUD Regional and Field Offices will be trained to understand and comply with the policy and procedures enunciated in this *Handbook* through a program of continuing education and training covering all facets of the security measures in effect within the respective offices. Such education and training will be accomplished on an individual, small group, or “all hands” basis. The scope of the education and training program will be based on the provisions of the local Physical Security Plan and OEP and will entail: a new employee security orientation; functional training; specialized training; an annual update; and tests, drills, and exercises.

### **5.2 Training Objectives**

Security education and training for HUD Regional and Field Office managers, supervisors, and staff members will be tailored to accomplish the following objectives:

- Ensuring that physical security considerations are an integral part of all office mission and support activities;
- Establishing and maintaining an attitude of individual and collective safety and security awareness within the office at all times;
- Ensuring that all employees understand their individual and collective responsibilities for implementation of the office Physical Security Plan and the OEP; and
- Providing a means for resolving any issues or questions that may arise concerning the physical security measures in effect within the office and its environs.

### **5.3 New Employee Orientation**

Each new Regional or Field Office employee will receive an initial orientation on office security procedures and the responsibilities of each individual for maintaining security. It is anticipated that “security” will be only one portion of a comprehensive new employee orientation that will cover all aspects of office operations, including local managerial, administrative, and logistical policy and procedures. The topics to be included in the security portion of the new employee orientation briefing, which should be presented by the Office Security Coordinator, are shown in Figure 5-1. This briefing may be augmented by a handout (fact sheet) that summarizes key aspects of the office security measures covered in the briefing.

### **5.4 Security Training**

In addition to the new employee orientation described above and summarized in Figure 5-1, the Office Security Coordinator will oversee and implement a comprehensive security training program for the office that covers functional training, specialized training, and an annual update. Each of these training activities is briefly described in the following sub-sections.

The actual conduct of the training may take the form of a briefing, group discussion, and/or workshop. A comprehensive security training, education, and awareness program of instruction, plus applicable training materials as appropriate, will be developed and distributed to all concerned by the Physical Security Division, OSEP. Field training will be provided by the Department of Homeland Security, Federal Protective Service.

**Figure 5-1 - Contents of New Employee Security Orientation Briefing**

- **Definition and importance of physical security**
- **Site orientation, including available communications and local support services available**
- **Highlights of Office Physical Security Plan**
- **Pertinent information concerning facility and environs**
  - **Perimeter security**
  - **Entry security**
  - **Interior security**
  - **Coordinating instructions**
- **Highlights of Occupant Emergency Plan**
  - **Occupant Emergency Organization**
  - **Building information**
  - **Procedures for specific emergencies (e.g., workplace violence)**
  - **Emergency evacuation procedures**
  - **Shelter-in-place procedures**
- **Individual and collective responsibilities**
- **Key contacts and telephone numbers**

#### **5.4.1 Functional Training**

It is essential that the HUD Regional and Field Office physical security training and education program includes each of the major functions that must be addressed in order to ensure that each employee has the understanding and knowledge to assure a safe and secure working environment. Such functions, which should be covered in the local Physical Security Plan and OEP, include:

- Provisions for facility security—external, at entrances and exterior doors, and internal;
- Provisions for individual and collective workplace safety;
- Local security procedures such as access control and display of individual ID badges;
- Protection and safeguarding of key assets, such as personnel files and information systems;
- Visitor control;
- Responsibilities of and interactions with the local security force, if applicable;
- Emergency evacuation procedures;
- Emergency and/or disaster response procedures (e.g., a bomb threat or actual attack with hazardous agents);
- Shelter-in-place conditions and procedures; and
- Emergency reporting and notification procedures, including key telephone numbers.

Functional training may be accomplished either in blocks of one or several related functions or in an omnibus session covering all of the functions, as determined to be most beneficial by the Office Security Coordinator. Participation in physical security functional training is mandatory for all HUD Regional and Field Office employees. If individuals are unable to attend the training session(s) at the time it is presented, the Office Security Coordinator must schedule and conduct a make-up session(s) within three months.

#### **5.4.2 Specialized Training**

Any time a new system, program, operating procedure, or item of equipment is introduced into the office, the Security Coordinator will determine the extent to which a modification in existing security procedures is necessary, or whether new, added security procedures need to be established. If a significant modification or addition to office security procedures is required, the Security Coordinator will take steps to modify the Office Physical Security Plan and/or the OEP, as appropriate, develop and/or arrange for the development of the requisite training materials, and schedule the conduct of the training for those occupants who are affected or involved. Depending on the nature or complexity of the material to be covered, specialized training may be conducted by subject-matter experts under the direction of and/or in coordination with the Office Security Coordinator.

#### **5.4.3 Annual Update**

An update on office physical security measures and emergency evacuation procedures in effect will be conducted for all employees on an annual basis. The scope of such training will cover the same topics as listed in Figure 5-1 for the new employee orientation briefing and will include any changes that may have occurred during the year since the previous annual training session(s). The training may be conducted for all employees at one time, or it may be scheduled, depending on availability or conflicting requirements, in several sessions to ensure that all personnel may avail themselves of the training commensurate with individual work schedules. The Office Security Coordinator will develop and publish the training schedule and present the training.

#### **5.4.4 Training Records**

The Security Coordinator will prepare a sign-in (i.e., attendance) sheet for each security training activity conducted in the office. These sheets will be retained on file to constitute a record of security training participation. Since training of all employees on security procedures is an important indicator of proper office security practices, these sign-in sheets will be made available to visiting physical security status assessment teams (e.g., QMR teams (see Section 4.7 in Chapter 4)) to validate the existence of a comprehensive local security-training program.

### **5.5 Tests, Drills, and Exercises**

As an adjunct to the training activities described, tests, drills, and exercises provide a means for evaluating the effectiveness of the training and support systems, as well as to test new concepts or operational procedures. Types of events to be considered are listed below.

- Communication tests. These events focus on the operational capabilities of communications and information systems that support mission operations. They should be conducted periodically (monthly as a goal) to ensure that all required systems are available and operational in response to an emergency situation.

- Emergency response, evacuation and shelter-in-place drills. These events enable staff members to practice the actual performance of emergency functions and provide an opportunity to evaluate the effectiveness of prescribed procedures in response to a simulated emergency situation.
- Tabletop exercises. Tabletop exercises provide participants an opportunity to analyze and discuss how best to deal with a simulated emergency in an informal, stress-free setting. They are designed to elicit constructive discussions concerning potential problem resolution based on implementation of existing plans. There are minimal equipment requirements, no deployment of resources, and no time pressures.
- Functional exercises. Functional exercises are fully simulated interactive events. They are intended to validate the capability of the office to respond to a simulated emergency in one or more of the functional areas identified above. These exercises may focus on policies, procedures, roles, and responsibilities of various entities before, during, and/or after an emergency event.
- Full-scale exercises. Full-scale exercises simulate, to the extent possible, actual emergency conditions. Such exercises are designed to evaluate the emergency response capabilities of the entire office staff in a highly stressful environment. This will generally include the full-time commitment for a prescribed period of time of office personnel, equipment, and resources to dealing with the simulated emergency at hand.

Each of the above events will be reviewed to determine the most beneficial in achieving an effective security posture for a given office, and how often they are conducted will be determined on a case-by-case basis. However, it is mandatory that each Regional and Field Office conduct at least one shelter-in-place drill and two building evacuation drills annually. For advice and assistance, the Office Security Coordinator should consult with the Physical Security Division, OSEP.

## **5.6 Security Awareness**

Security awareness on the part of occupants of each Regional or Field Office is critical to establishing a secure workplace to conduct business and ensure the safety of personnel and physical assets. The Office Director and Security Coordinator will work with all HUD employees to incorporate security awareness and reminders on a routine basis into the conduct of office staff meetings and briefings.

Many federal agencies have found it beneficial to periodically send out security-related messages with each message concentrating on a specific issue, such as reminders on how to identify and handle suspicious packages. In some cases, posters may be used to reinforce such reminders (e.g., the U.S. Postal Service poster on suspicious mail). While much information can be distributed via e-mail, this may result in e-mail “overload,” which could have a negative effect. An alternative might be desk-to-desk distribution of brightly colored fact sheets (using the same color for all security-related material), along with the use of in-house newsletters and publications. OSEP will periodically provide, on the hud@work Intranet website, security information and reminders for HUD staff members both in Headquarters and in the field. Regional and Field Offices with similar internal web pages are encouraged to do the same.

Office Security Coordinators should look for a variety of means to foster security awareness throughout the office. For example, extracts from the office’s OEP and Physical Security Plan

could be posted prominently in the office's reception area, the employees' lounge/lunch room, or in other areas where employees/visitors congregate. These documents in their entirety might also be posted on the hud@work Intranet website and/or a similar local intranet web page. For advice and assistance concerning this matter, Office Security Coordinators should contact the Physical Security Division, OSEP.

# Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Appendix A - Security Standards for Leased Space

#### A.1 Leased Space Security Standards Overview

The standards established by the Department of Justice (DOJ) report, *Vulnerability Assessment of Federal Facilities*, dated June 28, 1995 (reference 1.4a in Chapter 1) were intended to provide guidelines to be followed for all federally occupied facilities. However, it became apparent that these standards were not readily applicable to most leased locations. Therefore, the Interagency Security Subcommittee (ISC), created by Executive Order 12977, established a subcommittee to develop a distinct set of standards specifically for leased facilities.

These standards are presented in the ISC Subcommittee Final Report, *Security Standards for Leased Space*, dated May 16, 2003 (see reference 1.4h in Chapter 1).

Physical security standards for HUD facilities, in both leased and Federal facilities, are provided in Chapters 2 and 3. This Appendix provides information on administrative procedures and new construction in leased space, because the procedures differ from those in Federal facilities.

#### A.2 Leased Space Administrative and New Construction Security Standards – Level I or II Facility

Following are leased space administrative procedures and new construction details concerning security standards for leased space in a Level I or II federal facility

#### LEASED SPACE ADMINISTRATIVE PROCEDURES – LEVELS I AND II

| Elements                                  | Standards   |
|---|---|
| <b>a. Occupant Emergency Plans (OEPs)</b> | Building managers and owners are required to cooperate with and participate in the development and implementation of government OEPs.   |
| <b>b. Background security checks</b>      | Conduct background security checks and/or establish security control procedures for contract service personnel as deemed necessary.   |
| <b>c. Security upgrade provisions</b>     | The government reserves the right, at its own expense and with its own manpower, to temporarily upgrade security during heightened alert conditions due to emergency situations such as terrorist attacks, natural disasters, and/or civil unrest. The measures shall be in accordance with the latest version of the HSAS. |

**LEASED SPACE NEW CONSTRUCTION – LEVELS I AND II**

| Type of Facility                        | Blast/Setback Standards   |
|---|---|
| <b>A. Any Level I federal facility</b>  | 20-foot setback, which is the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion), with appropriate window glazing. For this level, there is no blast load standard, glazing performance condition, nor facade protection level requirement.   |
| <b>B. Any Level II federal facility</b> | 20-foot setback, which is the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion), with appropriate window glazing. Glazing performance should provide for a “high” protection level and “low” hazard level (i.e., glazing cracks and fragments may enter interior space and land on the floor not farther than 10 feet from the window). Facade protection would be “medium,” which would result in moderate damage, but repairable. Some casualties may occur and assets may be damaged. |

**A.3 Leased Space Administrative and New Construction Security Standards – Level III Facility**

Following are leased space administrative procedures and new construction details concerning security standards for leased space in a Level III federal facility.

**LEASED SPACE ADMINISTRATIVE PROCEDURES – LEVEL III**

| Elements                                  | Standards   |
|---|---|
| <b>a. Occupant Emergency Plans (OEPs)</b> | Building managers and owners are required to cooperate with and participate in the development and implementation of government OEPs.   |
| <b>b. Background security checks</b>      | Conduct background security checks and/or establish security control procedures for contract service personnel as deemed necessary.   |
| <b>c. Security upgrade provisions</b>     | The government reserves the right, at its own expense and with its own manpower, to temporarily upgrade security during heightened alert conditions due to emergency situations such as terrorist attacks, natural disasters, and/or civil unrest. The measures shall be in accordance with the latest version of the HSAS. |

**LEASED SPACE NEW CONSTRUCTION – LEVEL III**

| Type of Facility                      | Blast/Setback Standards  |
|---------------------------------------|--|
| <b>Any Level III federal facility</b> | 20-foot setback, which is the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion), with appropriate window glazing. Glazing performance should provide for a “high” protection level and “low” hazard level, (i.e., glazing cracks and fragments may enter interior space and land on the floor not farther than 10 feet from the window). Facade protection would be “medium,” which would result in moderate damage, but repairable. Some casualties may occur and assets may be damaged. |

**A.4 Leased Space Administrative and New Construction Security Standards – Level IV Facility**

Following are leased space administrative procedures and new construction details concerning security standards for leased space in a Level IV federal facility.

**LEASED SPACE ADMINISTRATIVE PROCEDURES – LEVEL IV**

| <b>Elements</b>                           | <b>Standards</b>  |
|---|---|
| <b>a. Occupant Emergency Plans (OEPs)</b> | Building managers and owners are required to cooperate with and participate in the development and implementation of government OEPs.   |
| <b>b. Background security checks</b>      | Conduct background security checks and/or establish security control procedures for contract service personnel as deemed necessary.   |
| <b>c. Security upgrade provisions</b>     | The government reserves the right, at its own expense and with its own manpower, to temporarily upgrade security during heightened alert conditions due to emergency situations such as terrorist attacks, natural disasters, and/or civil unrest. The measures shall be in accordance with the latest version of the HSAS. |

**LEASED SPACE NEW CONSTRUCTION – LEVEL IV**

| <b>Type of Facility</b>                | <b>Blast/Setback Standards</b>  |
|--|---|
| <b>a. Non-law enforcement agencies</b> | 50-foot setback, which is the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion), with appropriate window glazing. Glazing performance should provide for a “high” protection level and “low” hazard level, (i.e., glazing cracks and fragments may enter interior space and land on the floor not farther than 10 feet from the window). Facade protection would be “medium,” which would result in moderate damage, but repairable. Some casualties may occur and assets may be damaged.  |
| <b>b. Child care facilities</b>        | 50-foot setback, which is the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion), with appropriate window glazing. Glazing performance should provide for a “very high” protection level and hazard level of “none,” (i.e., glazing is cracked but is retained by the frame, and dusting or very small fragments may occur near the window sill or on the floor). Facade protection would be “higher,” which would result in minor damage, but repairable. Occupants may incur some injury, and assets may receive minor damage.  |
| <b>c. Law enforcement agencies</b>     | 100-foot setback, which is the distance from the face of the building’s exterior to the protected/defended perimeter (i.e., any potential point of explosion), with appropriate window glazing. Glazing performance should provide for a “very high” protection level and hazard level of “none,” (i.e., glazing is cracked but is retained by the frame, and dusting or very small fragments may occur near the window sill or on the floor). Facade protection would be “higher,” which would result in minor damage, but repairable. Occupants may incur some injury, and assets may receive minor damage. |

**A.5 Leased Space Security Standards – Level V Facility**

HUD does not currently occupy leased space in any Level V facility.

# Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Appendix B - HUD Office Physical Security Plan

The suggested organization and content of a HUD Office Physical Security Plan are illustrated in Figure B-1. The overall objective of the Plan is to **fully delineate the procedures to be followed and systems and equipment employed** to ensure the safety and protection of the personnel, information, equipment, and materials located in the office and to preclude unauthorized access to the facility. Only those portions of the outline in Figure B-1 that apply to a given facility should be included in the Office Physical Security Plan.

Each Office Physical Security Plan will be tailored to the Federal Security Level of the office, the minimum HUD security standards that apply, the characteristics of the facility (i.e., either federal or leased space), and the environment in which the office is located. A brief description of the contents of the Plan is as follows:

#### Part 1. Introduction

Delineate the purpose of the Plan, plus applicability and scope, authorities, references, and security responsibilities of key officials and other occupants of the office.

#### Part 2. Pertinent Information

##### 2.1 Description of Facility

Describe all aspects of the facility that clearly portray the setting and environment in which the office is located, including other occupants of the building, proximity of parking areas, number and location of entrances/exits, etc.

##### 2.2 Description of Surrounding Area

Identify the nature of external activities that adjoin the boundaries of the facility in each direction. Include any potential areas of concern relative to the facility and its occupants.

##### 2.3 Proximity to Emergency Services

Identify and indicate the location and estimated response times of local law enforcement, fire and rescue, hazardous materials (HAZMAT) response, and emergency medical service facilities and organizations.

##### 2.4 Facility/Office Physical Security Organization

Describe the physical security organization of the office and the facility as a whole, including location of security force posts, duty hours, and emergency equipment available.

##### 2.5 Key Telephone Numbers

Provide a list of key telephone numbers, both internal and external.

### Part 3. Perimeter Security

Describe the measures taken to provide perimeter security, including physical barriers, parking area access and controls, exterior lighting, video surveillance, security control posts, shatter-resistant windows, etc.

### Part 4. Entry Security

Describe the procedures and equipment/systems employed to control and monitor the entry of personnel, mail/packages, and other items into the building in which the HUD office is located and into HUD office space itself.

### Part 5. Interior Security

Describe the measures taken to provide interior security within the building in which the HUD office is located and within HUD office space itself, including controlling access to critical or sensitive areas, designated mail/package handling areas and procedures, mandatory display of ID badges/visitor passes, etc.

### Part 6. Coordinating Instructions

Describe the general policies and procedures in effect to ensure the safeguarding and protection of all personnel, information, equipment, and materials within the HUD office, including trash disposal procedures, key/combination controls, communications/ computer systems security, incident reporting, coordination with other local federal agencies, and security training, education, and awareness for all employees.

**Figure B-1. Outline of HUD Office Physical Security Plan**

| <b>OFFICE PHYSICAL SECURITY PLAN</b>                                |  |
|---|--|
| <b>Part 1. Introduction</b>   |  |
| <b>1.1 Purpose</b>  |  |
| <b>1.2 Applicability</b>  |  |
| <b>1.3 Scope</b>  |  |
| <b>1.4 Authorities</b>  |  |
| <b>1.5 References</b>   |  |
| <b>1.6 Security Responsibilities</b>                                |  |
| <b>Part 2. Pertinent Information</b>                                |  |
| <b>2.1 Description of Facility</b>                                  |  |
| <b>2.1.1 General</b>  |  |
| <b>a. Federal Security Level</b>                                    |  |
| <b>b. Leased or Federal</b>   |  |
| <b>c. Office Population</b>   |  |
| <b>d. HUD Office Space (square feet)</b>                            |  |
| <b>2.1.2 Building Occupants (other than HUD)</b>                    |  |
| <b>2.1.3 Parking Areas</b>  |  |
| <b>2.1.4 Entrances/Exits</b>  |  |
| <b>2.1.5 Elevators/Stairwells</b>                                   |  |
| <b>2.1.6 Alarm and Public Address Systems</b>                       |  |
| <b>2.1.7 Normal Duty Hours</b>                                      |  |
| <b>2.2 Description of Surrounding Area</b>                          |  |
| <b>2.2.1 Activities/Structures Immediately Adjacent to Facility</b> |  |
| <b>2.2.2 Potential Areas of Concern</b>                             |  |
| <b>2.3 Proximity to Emergency Services</b>                          |  |
| <b>2.3.1 Law Enforcement</b>  |  |
| <b>2.3.2 Fire Department</b>  |  |
| <b>2.3.3 Hazardous Materials Response</b>                           |  |
| <b>2.3.4 Emergency Medical Services</b>                             |  |

**Figure B-1. Outline of HUD Office Physical Security Plan (continued)**

**Part 2. Pertinent Information (continued)**

**2.4 Facility/Office Physical Security Organization**

**2.4.1 Size and Composition of Security Force**

**2.4.2 Post Locations and Duty Hours**

**2.4.3 Equipment Available (e.g., radios, firearms, riot gear, handcuffs, emergency medical equipment, etc.)**

**2.5 Key Telephone Numbers**

**2.5.1 Internal**

**2.5.2 External**

**Part 3. Perimeter Security**

**3.1 General**

**3.2 Physical Barriers**

**3.3 Parking Area Access and Controls**

**3.4 Exterior Lighting**

**3.5 Signage**

**3.6 Closed Circuit Television (CCTV) Surveillance and Monitoring**

**3.7 Perimeter Security Control Post(s)**

**3.8 Security Patrols**

**3.9 Shatter-resistant Windows**

**Part 4. Entry Security**

**4.1 General**

**4.2 Building Access Control and Monitoring**

**4.2.1 Main Entrance**

**4.2.2 Other Entrances/Exits**

**4.2.3 Shipping/Receiving Areas**

**4.2.4 CCTV**

**4.2.5 After Hours Procedures**

**4.3 HUD Office Space Access Control and Monitoring**

**4.3.1 Entry Control**

**4.3.2 Government Rules and Regulations**

**4.3.3 Mail and Package Handling**

**4.3.4 Entry Area CCTV Surveillance**

**Figure B-1. Outline of HUD Office Physical Security Plan (continued)**

**Part 4. Entry Security (continued)**

**4.3.5 High Security Locks**

**4.3.6 Unauthorized Entry Intrusion Detection System(s)**

**Part 5. Interior Security**

**5.1 General**

**5.2 Building Interior Security**

**5.2.1 Access to Utility Areas**

**5.2.2 Heating, Ventilation, and Air Conditioning (HVAC)**

**5.2.3 Emergency Back-up Power for Critical Systems**

**5.2.4 Public Restroom Access and Security**

**5.3 HUD Office Space Interior Security**

**5.3.1 Reception Area**

**a. Configuration**

**b. Duress Alarm**

**5.3.2 Employee ID Display and Control**

**5.3.3 Visitor ID/Pass Display and Control**

**5.3.4 Mail and Package Handling Procedures**

**5.3.5 Shipping/Receiving Area(s)**

**5.3.6 Access to Sensitive or Controlled Access Area(s)**

**5.3.7 Internal Intrusion Detection System(s)**

**Part 6. Coordinating Instructions**

**6.1 Administrative Policies/Procedures**

**6.1.1 Information Security**

**6.1.2 Trash Disposal**

**6.1.3 Authorized Personnel Access List**

**6.1.4 Keys/Key Cards/Combination Controls**

**6.1.5 Security Provisions in Lease Agreements**

**6.1.6 Building Security Committee**

**6.2 Communications /Computer Systems Security**

**6.3 Background Security Checks of Maintenance/Custodial Personnel**

**Figure B-1. Outline of HUD Office Physical Security Plan (*continued*)**

**Part 6. Coordinating Instructions (*continued*)**

**6.4 Contingency Readiness and Reporting**

**6.4.1 Malfunctioning Systems or Equipment**

**6.4.2 Incident Reporting**

**6.4.3 Threat Monitoring**

**6.5 Security Measures—Occupant Emergency Plan (OEP)**

**6.6 Coordination with Other Local Federal Agencies**

**6.7 Security Training, Education, and Awareness**

**Department of Housing and Urban Development**  
**Physical Security Handbook for HUD Regional and Field Offices**

**Appendix C - Occupant Emergency Program**

**C.1 General**

An **Occupant Emergency Program** that establishes procedures for safeguarding lives and property in and around a facility during an emergency is mandatory for all HUD field activities. The emergency may include: a fire; explosion; discovery of an explosive device; actual or potential exposure to hazardous substances; severe weather; a natural disaster, such as a hurricane or earthquake; chemical, biological, or radiological threat or exposure; hostage takeover; or physical threat to the building, occupants, or visitors.

An effective Occupant Emergency Program for HUD field activities will include the following essential elements:

- Assignment and delineation of **emergency responsibilities** to individuals who have been designated to undertake certain responsibilities and perform specific tasks in response to an incident or event that threatens a facility and/or its occupants. This will be achieved by establishment of an **Occupant Emergency Organization (OEO)**, which is described in Section C.2 below;
- Provision to all occupants of specific **information about the building's construction and layout**, as well as identification of all tenants in the building. This can be accomplished through a "Building Information Sheet" and "Occupant Information Sheet." Floor plans, entrances/exits, and evacuation routes should be clearly marked. This information should be included in the **Occupant Emergency Plan (OEP)** (see Section C.3 below) for the facility;
- A listing of key **emergency telephone numbers** that is available to every occupant in the building. One way to ensure that everyone has and keeps a copy is to publish the list in the local federal telephone directory, preferably on the inside of the front cover or on the first page. Also, the listing can be posted on the Intranet (HUD@work) site for the HUD office employees. The list should also be published in the **OEP**;
- Designation of an **Emergency Command Center (ECC)**, which will be activated to provide direction and control of emergency response personnel and activities. The ECC should be centrally located and easily accessible, with sufficient communications, including, if possible, portable radios and pagers, to enable timely contact with all concerned in response to the emergency. Messengers should be available to augment communications systems. Planning should provide for an alternate ECC in the event that the main one is incapacitated or otherwise unavailable;
- Delineation of **response procedures for different types of emergencies** that may typically be encountered in or in the vicinity of the facility. Such emergency situations may include a fire, power outage, exposure or potential exposure to hazardous substances, presence of a suspicious object or explosive device, a medical emergency, etc. For each of these situations, it is desirable that a checklist be prepared that delineates proper response procedures such as: immediate action(s) to be taken; alarm activation, if

applicable; reporting and notification requirements; key telephone numbers; and location of emergency response personnel or expertise (e.g., HAZMAT teams); and

- Assignment of duties and responsibilities to designated individuals for assisting mobility-impaired persons or persons with disabilities during building evacuations or shelter-in-place procedures in connection with drills, exercises, or actual emergencies. Recommended support equipment and systems for all Regional and Field Offices include:
  - Telecommunications Devices for the Deaf (TDD);
  - Strobe lights;
  - Emergency evacuation chairs; and
  - Notification protocol via a “Direct Alert” message to all employee computers.

## **C.2 Occupant Emergency Organization (OEO)**

An **OEO** is a group of employees assigned to undertake certain responsibilities and perform specific tasks in preparation for and response to an emergency that threatens a facility and/or its occupants. The OEO operates under the direction of an individual identified as the **Designated Official (DO)**. The DO is the highest-ranking federal official in the facility, or another person agreed on by all tenant agencies.

The OEO generally consists of an **Emergency Command Center Team (ECCT)**, **Floor Teams**, and a **Damage Control Team**. Guidelines for setting up the organization include:

- The organization should be limited in size, with only the number of positions required to deal with the emergencies anticipated and clearly defined duties for each position. It is important to have enough help in any emergency, but too many people could get in the way and inhibit rapid, efficient response;
- To the extent possible, the organization should consist of and use the existing hierarchy of the occupant agencies. Ideally, the same officials who run the agencies on a day-to-day basis should assume leadership positions during an emergency; and
- Emergency organization members should be identified by position, not by name. This will allow for continuity since someone normally is designated to fill a position when the incumbent is absent. Thus, the acting official will assume the incumbent’s role when an emergency occurs.

### **C.2.1 Emergency Command Center Team (ECCT)**

The ECCT will prepare, plan for and direct all emergency operations from the centrally located ECC. In a large facility, composition of the ECCT will include: the Designated Official (DO), an Occupant Emergency Coordinator (OEC), a Floor Team Coordinator (FTC), a Damage Control Team Coordinator (DCTC), a Medical Coordinator, an Administrative Officer, and Technical Advisors. In a small facility, some positions, such as an FTC, Medical Coordinator, and Administrative Officer, may not be needed, or one person could perform several functions.

Special consideration should be given to timely notification of ECCT members of an emergency and rapid deployment of Team members from their workstations to the ECC.

A description of the duties and responsibilities of individual ECCT members is shown in Figure C-1.

**Figure C-1. Duties and Responsibilities of Emergency Command Center Team (ECCT) Members**

|  |
|--|
| <p><b>Designated Official (DO)</b></p> <ul style="list-style-type: none"><li>▪ Coordinates with all tenants and develops an OEP.</li><li>▪ Selects and trains OEO members.</li><li>▪ Ensures that appropriate procedures are followed during emergencies.</li><li>▪ Identifies and establishes working relationships with federal, state, and local agencies that might respond to an emergency in the facility.</li><li>▪ Initiates activities to prepare occupants for emergencies and inform them of response procedures.</li></ul> <p><b>Occupant Emergency Coordinator (OEC)</b></p> <ul style="list-style-type: none"><li>▪ Acts for the DO during absences.</li><li>▪ Performs delegated duties of the DO.</li><li>▪ Serves as liaison between the DO and other members of the ECCT.</li></ul> <p><b>Floor Team Coordinator (FTC)</b></p> <ul style="list-style-type: none"><li>▪ Coordinates the planning of occupant movement between floors during an emergency.</li><li>▪ Coordinates floor, wing, stairwell, elevator, and other monitor activities within the facility.</li></ul> <p><b>Damage Control Team Coordinator (DCTC)</b></p> <ul style="list-style-type: none"><li>▪ Identifies and monitors the operation and condition of utilities, alarm systems, communications equipment, and other pertinent systems and equipment in the facility.</li><li>▪ Makes recommendations on the use of available equipment and systems during an emergency.</li><li>▪ Maintains emergency call list for malfunction of utilities and presence of hazardous substances.</li><li>▪ Directs Damage Control Team activities.</li></ul> <p><b>Medical Coordinator (MC)</b></p> <ul style="list-style-type: none"><li>▪ Identifies and maintains a list of available medical emergency services.</li><li>▪ Maintains first aid equipment.</li><li>▪ Arranges for cardiopulmonary resuscitation (CPR), first aid, and other paramedical training.</li><li>▪ Maintains a list of personnel with CPR, first aid, and paramedical training within the facility.</li></ul> <p><b>Administrative Officer (AO)</b></p> <ul style="list-style-type: none"><li>▪ Provides required administrative services (phones, faxes, radios, pagers, etc.) and prepares reports.</li><li>▪ Prepares and maintains OEO records and updates them monthly.</li></ul> <p><b>Technical Advisors</b></p> <p><b>Building Manager (BM)</b></p> <ul style="list-style-type: none"><li>▪ Maintains and provides to the DO, OEC, and DCTC information about the building and the operation of its mechanical systems.</li></ul> <p><b>Physical Security Specialist (PSS)</b></p> <ul style="list-style-type: none"><li>▪ Provides advice on building security and law enforcement matters.</li><li>▪ Serves as liaison with federal and local law enforcement agencies.</li></ul> <p><b>Other Tenants</b></p> <p>Maintain liaison with the DO; provide information, advice, and/or assistance, as appropriate, concerning unique emergency response capabilities or requirements.</p> |
|--|

**C.2.2 Floor Teams (FTs)**

Emergency response actions in accordance with the local OEP are, for the most part, carried out by Floor Teams (FTs) assigned to (and in between) each floor of a facility. A typical FT

in a large facility would include: a Floor Monitor (FM); Wing or Area Monitors (one for each major area on a floor); Stairwell Monitors; Elevator Monitors; Monitors for Persons with Disabilities; and Exit Monitors (at street and ground level). All monitors will work with and cooperate with each other, particularly in the evacuation of persons with disabilities. (Small or single-story facilities will probably not need separate persons for all of these monitoring functions. In this case, duties and responsibilities will be combined and apportioned out to a smaller number of Floor Team members.)

Duties and responsibilities of Floor Team members are described in Figure C-2.

**Figure C-2. Duties and Responsibilities of Floor Team Members**

**Floor Monitors (FMs)**

- Maintain communication with the FTC during an emergency; provide progress reports on evacuation or shelter-in-place activities; for evacuation, notify the FTC when a floor is completely cleared.
- Designate exact boundaries of floor areas and assign responsibility for these areas.
- Coordinate necessary changes in floor organization with the FTC and OEC.
- Ensure that evacuation routes are known to occupants and are clearly identified and posted on bulletin boards, corridor intersections, and office exits.

**Wing or Area Monitors**

- Notify the FM when an area has been completely cleared, or when shelter-in-place actions have been completed.
- Ensure that evacuation routes are made known to occupants and are clearly identified.
- During drills and emergencies, direct the orderly flow of persons along prescribed evacuation routes or shelter-in-place routes, as applicable.
- When required, ensure the complete evacuation of the wing or area.
- During fire evacuations, ensure that windows and doors are left closed, lights are on, and electrical appliances are off.
- During bomb threat evacuations, leave windows and doors open and lights on.
- Supervise Stairwell Monitors and Monitors for Persons with Disabilities.
- Maintain and provide to the FM a current list of persons with disabilities (including name, telephone number, room number, and type of disability).
- Assign Monitors for persons with disabilities, one per disabled person.

**Stairwell Monitors**

- If evacuation is required because of a bomb threat, search assigned stairwell; and report findings to the Wing or Area Monitor.
- Control movement of personnel in assigned stairwell, keeping them in a single file and moving steadily at a walking pace; instruct personnel to grasp handrails.
- Keep door to the stairwell open until the wing or area is clear.
- Restrict and monitor use of assigned stairwell (and escalator, if present), as necessary.
- Know the locations and telephone numbers of persons with disabilities who will require assistance, types of disabilities, and location of crutches, wheelchairs, and other support devices.
- Know the location and telephone number of the Monitor for Persons with Disabilities who has been assigned to each disabled person.
- With the designated Monitors for Persons with Disabilities, assist disabled persons in evacuating the building using the assigned stairwell.

**Elevator Monitors**

- Be familiar with the provisions of GSA bulletins covering emergency plans for using elevators to evacuate persons with disabilities.
- Be familiar with the manual operation of elevators.
- Take charge of the use of assigned elevator(s), and permit use only as directed by the FM.
- During fire evacuation, direct personnel attempting to use the assigned elevator(s) to the appropriate stairwell; relinquish control of the elevator(s) to firefighting personnel when they arrive.
- If emergency response personnel are arriving by elevator, meet them and direct them to the scene of the

emergency.

- Know the location and telephone number of the Monitor for Persons with Disabilities who has been assigned to each disabled person.
- With the designated Monitors for Persons with Disabilities, assist disabled persons in evacuating the building by elevator, if the elevator has been approved for use.

### **Figure C-2. Duties and Responsibilities of Floor Team Members (*continued*)**

#### **Elevator Monitors (*continued*)**

- If the elevator cannot be used for evacuation help the Monitor for Persons with Disabilities assist his/her assigned disabled person to the vicinity of the nearest safe stairwell.

#### **Monitors for Persons with Disabilities**

- Know the location and telephone number of the disabled person to whom assigned, type of disability, and location of crutches, wheelchairs, and other support devices.
- With the designated Stairwell or Elevator Monitor, assist the disabled person in evacuating the building using either the assigned stairwell or elevator.

#### **Exit Monitors**

- Ensure that exits are open and free of hindrances.
- Deny unauthorized access to the building.
- Direct orderly movement of evacuating personnel to designated safe areas.
- Assist in the evacuation of persons with disabilities, as necessary.

### **C.2.3 Damage Control Team**

The Damage Control Team consists of the Building Manager and other people familiar with the facility's construction, equipment, and operating systems. Team members will report to and carry out emergency functions under the direction of the DCTC. Generally, their job is to control dangerous conditions until further help arrives and to assess potential and real danger. This involves preparing and planning for dangerous conditions, especially those most likely and/or most harmful. This may include duties such as:

- Ensuring that the appropriate response organization(s) (e.g., fire and rescue, law enforcement, medical, hazardous materials) has been notified;
- Assisting emergency response personnel;
- Disconnecting utilities or equipment;
- Conducting a bomb search;
- Performing initial rescue and first aid;
- Making emergency repairs; and
- Protecting records and equipment, and removing or isolating hazardous substances.

### **C.2.4 EO Special Considerations**

Establishment of an effective OEO must take into consideration designation of an alternate DO, timely and responsive communications, and actions concerning child care centers if present.

#### **C.2.4.1 Alternate DO**

In the absence of the designated DO, it is imperative that someone be in charge of the ECCT in the event of an emergency. Thus, an alternate DO must be identified – this may be more than one senior official who should be prepared to assume the duties of the DO should he/she be absent or unavailable.

A special case may be an emergency that occurs at night, over the weekend, or on a holiday. For this situation, the senior federal official present or most readily available should act as the DO and initiate appropriate response actions. Considerations include coordination with on-site Federal Protective Service personnel, if applicable, or contract security officers and after-hours maintenance personnel.

#### **C.2.4.2 Communications**

Of high priority concern to members of the OEO are the primary and alternate means of communication that will be used to:

- Activate the ECCT;
- Inform building occupants of the nature of the emergency and what actions to take; and
- Coordinate response activities during the emergency.

All occupants must know the location of fire alarm boxes and how and when to use the alarm in the event of a fire. Occupants should also know whom they should notify after turning in an alarm so that the ECC can be activated. For other emergencies, telephones, public address systems, and/or messengers should be employed to notify and contact members of the OEO and other building occupants.

If telephones are to be used, the AO should act as “communications coordinator,” or appoint someone else to do so, so that all members of the OEO and other occupants may be contacted in a timely manner. For this eventuality, the AO should prepare in advance, and keep current, a comprehensive list of key telephone numbers.

Some multilevel buildings may have emergency telephone systems (e.g., “red” telephones) for coordinating emergency response activities. In their absence, however, OEO members should be prepared to rely on the normal telephone system, public address system, and/or messengers.

#### **C.2.4.3 Child Care Centers**

If a child care center is collocated in a facility where a HUD office is located, the DO and Physical Security Specialist should work with the director of the child care center to develop and display emergency response procedures. Staff personnel assigned to the child care center should know whom to contact in the event of a medical emergency, how the center will be notified of a fire or other hazard that may require evacuation, the location of fire alarm boxes and fire extinguishers, primary and secondary evacuation routes, and the location of safe areas.

Child care center staff management and personnel should be encouraged to develop a system for accountability of all children and staff in the center at all times and to conduct

practice evacuation and shelter-in-place drills so that children will not be unprepared or unduly alarmed should a real emergency occur.

### C.3 Occupant Emergency Plan (OEP)

An **OEP** is a set of procedures designed to protect life and property in federally-occupied space under emergency conditions. The primary objectives of an OEP are to:

- Minimize the impact of emergencies upon the safety and well-being of personnel;
- Protect government assets against loss or damage;
- Provide for the timely, orderly, and safe evacuation of the building; and
- Provide instructions for shelter-in-place situations.

The OEP will be published as an attachment to a directive entitled “Occupant Emergency Plan for (Name of Facility)” addressed and distributed to all tenant agencies in the facility in which the HUD office is located. Affixed to the directive will be a Responsible Officials’ Sign-Off Sheet that contains the date and signature of the:

- Designated Official who heads the OEO for the facility;
- Building Manager;
- Senior Ranking Official of each of the tenant agencies located in the facility; and
- Designated Occupant Emergency Coordinator for the facility.

The heading of the sign-off sheet will contain a paragraph reading:

“By their signatures below, the following officials certify that they have participated in the development of the attached Occupant Emergency Plan and fully understand the procedures to be followed in an emergency affecting the facility and employees for which they are responsible.”

A suggested outline of an OEP is shown in Figure C-3.

Following is a description of the contents of each of the major portions of the HUD office OEP shown in Figure C-3.

- 1.0 Introduction.** This section of the OEP will clearly state its purpose and its applicability and scope (i.e., a description of the facility(ies) and agency(ies) to which it applies).
- 2.0 Preparatory Actions.** This section of the OEP will summarize general information concerning the actions taken prior to an emergency to ensure that all concerned understand key elements of OEP implementation and are prepared to fulfill their respective responsibilities.
- 2.1 Occupant Emergency Organization (OEO).** This section of the OEP summarizes the organization, composition, and responsibilities of the OEO (as described in Section F.2 above) established to deal with various emergency situations that may threaten or have an adverse impact on the facility and/or its occupants. This should include the location of the ECC.

- 2.2 Availability of OEP to all concerned.** The provisions of the OEP should be publicized and made available to all building occupants. In this regard, the OEP should be augmented by prominently-displayed visual aids (e.g., placards, signs, etc.) designed to assist occupants in dealing with emergencies within the facility. Ideally, an electronic version of the OEP should be available on each computer located at workstations throughout the facility.
- 2.3 Local emergency response agencies.** The OEP should identify and how to contact local emergency response agencies, such as law enforcement, fire and rescue, emergency medical services, and hazardous materials (HAZMAT) response teams (if separate from the local fire department). Prior coordination should be made with such agencies to ensure that up-to-date and accurate phone numbers and realistic response times are reflected in the OEP.
- 2.4 Training and drills.** The OEP should describe the types of training events and drills to be conducted to ensure the understanding of all concerned of their responsibilities in emergency situations. Local emergency response agencies should be included in the training and drills to the extent feasible. Further, the OEP should stipulate that participation by all building occupants in such events is mandatory.

**Figure C-3. Outline – HUD Office Occupant Emergency Plan (OEP)**

|                                       |                   |                                   |
|---------------------------------------|-------------------|-----------------------------------|
| 1.0 Introduction.                     |                   |                                   |
| Purpose, applicability, and scope     |                   |                                   |
| 2.0 Preparatory Actions               |                   |                                   |
| Occupant Emergency Organization (OEO) |                   |                                   |
| Availability of OEP to all concerned  |                   |                                   |
| Local emergency response agencies     |                   |                                   |
| Training and drills                   |                   |                                   |
| 3.0 Building Information              |                   |                                   |
| Layout and configuration              |                   | Sprinkler system                  |
| Floor plans                           |                   | Emergency lighting                |
| Equipment                             |                   | Elevators                         |
| Utilities                             |                   | Stairwells                        |
| Systems                               |                   | Entrances/exits/evacuation routes |
| Alarms                                |                   | Public address system             |
| 4.0 Emergency Telephone Numbers       |                   |                                   |
| 5.0 Emergency Response Actions        |                   |                                   |
| Bomb threat                           | Fire              | Suspicious package                |
| Power outage                          | Severe weather    | Medical emergency                 |
| Workplace violence                    | Civil disturbance | Other                             |
| 6.0 Emergency Evacuation Procedures   |                   |                                   |
| Before evacuation                     |                   |                                   |
| During evacuation                     |                   |                                   |
| Evacuation assembly area(s)           |                   |                                   |
| 7.0 Shelter-in-Place                  |                   |                                   |
| Shelter-in-place scenarios            |                   |                                   |

|  |
|--|
| <p>Shelter-in-place guidelines</p> <p>Shelter-in-place caveat</p> <p>Appendix A. Emergency Response Checklists</p> <p>Appendix B. Evacuation Routes</p> <p>Appendix C. Evacuation Assembly Area(s)</p> <p>Appendix D. Recommended Personal Emergency Kit</p> |
|--|

**3.0 Building Information.** The OEP should describe the layout and configuration of the building, including installed equipment, utilities, and systems. Floor plans and evacuation routes should be clearly marked. Specific information to be presented includes:

- Alarms.** Types of alarms and how activated;
- Sprinkler system.** Location(s) and how activated;
- Emergency lighting.** Location(s) and how activated;
- Back-up power.** Location(s) and how activated;
- Elevators.** Location(s) and restrictions on use, if any, during specific types of emergencies;
- Stairwells.** Location(s) and restrictions on use, if any, during specific types of emergencies;
- Entrances/exits.** Location(s) and restrictions on use, if any, during specific types of emergencies; and
- Public address system.** Who operates it, and when and how messages/information is injected.

**4.0 Emergency Telephone Numbers.** The OEP should include a listing of both internal and external telephone numbers to be used to:

- notify designated officials and/or key personnel of a specific type of emergency; and
- request specific assistance or support (e.g., fire department, law enforcement, medical/ambulance, etc).

Where applicable, the listing should indicate numbers to be used during normal duty hours and those that should be used after hours.

**5.0 Emergency Response Actions.** The OEP should identify specific types of emergencies (such as those listed in Figure C-3) that could occur in a federal facility and would require rapid, coordinated response. Detailed checklists for each type of emergency should be provided in Appendix A of the OEP (including who does what). General response actions and/or applicable services, equipment, or systems that are germane for each type of emergency are described below.

**5.1 Bomb threat.**

- a. Record time of receipt and exact wording of threat and (by separate phone, if required) report the threat to facility security force, chain of command, and 911.
- b. Conduct inspection of facility.
- c. Restrict access to facility.
- d. Evacuation, as determined to be necessary.
- e. Liaison with local law enforcement/fire department.

## **5.2 Fire.**

- a. Report to chain of command and local fire department.
- b. Activation and use of fire alarm system.
- c. Location and use of fire extinguishers.
- d. Local fire suppression system controls (e.g., sprinkler system).
- e. Evacuation, as determined to be necessary.
- f. Liaison with local fire department.

## **5.3 Suspicious package.**

- a. Upon initial sighting, report to chain of command.
- b. Public announcement to avoid designated area.
- c. Cordon off and restrict access to designated area.
- d. Evacuation, as determined to be necessary.
- e. Liaison with local fire department/HAZMAT team.

## **5.4 Power outage.**

- a. Automatic activation of uninterruptible power supply (UPS) for automated information systems and networks, if available.
- b. Within allotted time, turn off computers and shut down networks to salvage data.
- c. Activate emergency lighting and/or back-up power, as appropriate.
- d. Report to chain of command.
- e. If back-up power is not available, depending on the heating, ventilation, and air conditioning (HVAC) environment, consider evacuation, as appropriate.
- f. Liaison with local power company regarding the restoration of power.

## **5.5 Severe weather.**

- a. Differentiate between prior-warning and no-warning scenarios.
- b. Report to chain of command (may occur after public announcement in no-warning scenarios).
- c. Public announcement that occupants should avoid windows, doorways, and outer walls.

- d. Monitor local radio stations and TV weather channel.
- e. Employees and visitors should move to pre-designated areas of the building that offer the greatest protection (i.e., inner office spaces, and hallways and stairwells on the first floor).
- f. Consider evacuation to a hardened shelter, if available.
- g. Be prepared for power outage.

#### **5.6 Medical emergency.**

- a. Dispatch local trained first aid provider(s) to the scene.
- b. Administer first aid/CPR.
- c. Contact nearest emergency medical/health unit.
- d. Notify chain of command.
- e. Meet and brief responding medical unit.
- f. Arrange for ambulance and medical evacuation to health care facility, as necessary.

#### **5.7 Workplace violence.**

- a. May be caused by various circumstances, such as a disgruntled employee, jilted partner, or unhappy customer. Individual precautions include:
  - Staying out of the way;
  - Locking yourself in your office if you hear a commotion and/or gun shots and immediately calling 911 for law enforcement assistance;
  - Staying away from windows and doors; and
  - Waiting for an “all-clear” announcement before leaving your office.
- b. Permit the senior official present or member of the ECCT to deal with the situation, in accordance with local standard operating procedures.

#### **5.8 Civil disturbance.**

- a. Public announcement that occupants should remain within the building and avoid windows, doorways, and outer walls.
- b. Notification to chain of command, facility security force and local law enforcement.
- c. Remain in place until “all clear” announcement.

#### **5.9 Other.**

The location of the HUD office or local conditions may require that response actions for other emergencies (e.g., a hurricane, earthquake, etc.) also be stipulated in the OEP. A determination concerning the inclusion of information concerning the proper response to other emergencies of local concern should be made on a case-by-case basis.

#### **6.0 Emergency Evacuation Procedures.**

##### **6.1 Before evacuation.**

Preparations should be made to ensure that each occupant knows exactly what to do once an evacuation order is given. Information that should be prominently posted on each floor includes:

- By what means and by whom an order to evacuate the building is given;
- The location of and route(s) to the nearest exit for designated areas;
- Designated stairwells and/or elevators to be used;
- A reminder to all occupants to keep their individual ID badges on their person at all times; and
- Identification, location, and phone numbers of Floor Team members (see duties and responsibilities in Figure C-2 above).

Of particular importance is ensuring that Monitors for Persons with Disabilities and assigned disabled persons have gotten together in advance and understand the procedures to be followed in evacuating the building.

## **6.2 During evacuation.**

The OEP should include instructions to:

- Promptly respond to evacuation alarm/announcement;
- Remain calm;
- Vacate the building immediately, following the instructions of Floor Monitors, Wing or Area Monitors, Stairwell Monitors, Elevator Monitors, Security Officers, and other emergency response personnel;
- Be aware of and assist persons who may need help in evacuating the building;
- Ensure that evacuation of childcare center, if present, is carried out in a timely and orderly manner;
- Ensure accountability for and participation by all contractor personnel and visitors to the office in the evacuation process;
- Ensure proper use of stairwells and elevators (generally, stairs will be used by able-bodied personnel and elevators will be used by individuals with disabilities); and
- Once outside of the building, occupants should proceed directly to a designated evacuation assembly area. There may be more than one evacuation assembly area depending on the nature of the emergency or local situation.

## **6.3 Evacuation assembly area(s).**

The OEP should include the guidelines to:

- Designate the evacuation assembly area(s) and establish procedures to account for all personnel, in advance of need.
- Follow established procedures to account for all personnel, including contractors and visitors, who are in the designated evacuation assembly area(s) to ensure that the building has been completely evacuated; and

- Keep all personnel in the evacuation assembly area until the Designated Official, Floor Monitor, or other ECCT staff person has given an “all clear.”

## **7.0 Shelter-in-Place.**

Based on the nature of the threat, it may be safer in some instances for occupants to remain in the building rather than evacuate (i.e., to employ shelter-in-place).

### **7.1 Shelter-in-Place scenarios.**

Provisions should be made in the OEP for shelter-in-place as a protective action to minimize the chance of injury when an emergency situation such as one of the following occurs outside the building:

- Severe weather (high winds, tornado, hailstorm, etc.);
- Civil disturbance;
- Accidental chemical release due to an industrial/vehicle accident; and/or
- Chemical, biological, or radiological (CBR) event.

### **7.2 Shelter-in-Place guidelines.**

The duration of shelter-in-place can be as short as 15 minutes or in excess of 12 hours, depending on the situation. Shelter-in-place guidelines include:

- Employees should remain in their shelter-in-place location as designated in the OEP until information concerning the hazard or danger has been assessed and ECCT personnel have determined that it is safe for employees to exit the building;
- Occupants with workstations located next to a window should move to an inner corridor or office;
- Depending on the exterior hazard, building exterior entrances/exits may be secured and sealed, and HVAC air handlers and dampers shut down; and
- Public address announcements, or other means, will be used to periodically apprise occupants of the emergency situation and when it is safe to leave the building.
- Shelter-in-place drills should be conducted at least annually.
- Additional information on shelter-in-place guidelines can be found on the Centers for Disease Control website at <http://www.cdc.gov/niosh/topics/prepared/>.

### **7.3 Shelter-in-Place caveat.**

The OEP should indicate that shelter-in-place is a voluntary action, unless mandated otherwise by law enforcement or public health officials. Personnel who ask to leave the building before it has been determined to be safe to do so should be directed to the ECC where they will be informed of any civil restrictions. If no restrictions are in place, such personnel will be permitted to leave and escorted to a designated exit point. However, any persons leaving the building under such circumstances should be apprised of their individual responsibilities for any adverse effects resulting from their so doing.

## **Appendices.**

Following is a brief description of the information to be provided in each of the Appendices to the OEP.

### **Appendix A. Emergency Response Checklists**

For each of the emergency situations identified, Appendix A of the OEP should provide a detailed checklist that delineates actions to be taken by members of the ECCT and building occupants. The checklists should be used in planning and preparing for emergencies, and in drills and training exercises. An example of the information to be presented in such a checklist, in this case for a fire emergency, is shown in Figure C-4.

**Figure C-4. Emergency Response Checklist – Fire**

**Emergency Control Center Team (ECCT)**

All EECT members proceed to the ECC upon sounding of fire alarm or notification.

Individual response actions:

**Designated Official (DO)/Occupant Emergency Coordinator (OEC)**

- Activate ECCT.
- Verify fire department notification/response.
- Verify FPS (if applicable) or security force notification/response.
- Brief responding personnel.
- Coordinate response activities.

**Floor Team Coordinator (FTC)**

- Activate Floor Teams.
- Verify occupant status.
- Coordinate Floor Team activities.

**Damage Control Team Coordinator (DCTC)**

- Activate Damage Control Team.
- Determine building conditions (environmental/structural).
- Coordinate Damage Control Team activities.

**Medical Coordinator (MC)**

- Determine requirements for medical assistance.
- Coordinate medical assistance activities.

**Administrative Officer (AO)**

- Monitor and record alarm and notifications sequence.
- Record response activities.

**Floor Team (located on Fire Floor)**

**Floor Monitor**

- Activate fire alarm (if not already done).
- Supervise evacuation of occupants, ensuring that persons with disabilities are taken care of.
- Verify evacuation upon completion.
- Maintain contact with and report to FTC.

**Area Monitors**

- Direct evacuation of area occupants.
- Inspect area to ensure total evacuation.
- Coordinate evacuation of persons with disabilities.
- Maintain contact with and report status to Floor Monitor.

**Elevator Monitors**

- Direct occupants attempting to use elevators to the nearest safe stairwell.
- Assist in elevator evacuation of persons with disabilities if elevator use has been authorized.

**Stairwell Monitors**

- Inspect stairwell for smoke and other obstructions. If obstructed, direct occupants to another stairwell.
- Keep occupants moving in a single file down the stairwell.
- Maintain contact with and report status to Floor/Area Monitor.

**Monitors for Persons with Disabilities**

- Assist persons with disabilities in evacuating to designated evacuation assembly area.
- Report status to Floor/Area Monitor.

**Figure C-4. Emergency Response Checklist – Fire (continued)**

|   |
|---|
| <p><b>Floor Team (located on First Floor)</b></p> <p><b>Floor Monitor/Area Monitors</b></p> <ul style="list-style-type: none"><li>▪ Coordinate with and direct fire department personnel to fire floor.</li><li>▪ Restrict building access.</li><li>▪ Assist with occupant evacuation.</li></ul> <p><b>Elevator Monitors</b></p> <ul style="list-style-type: none"><li>▪ Maintain contact with and report to First Floor Monitor.</li><li>▪ Capture assigned elevators (either automatically or by using a special key, or by the regular call button).</li><li>▪ After capture, deny use of assigned elevators, unless authorized by the fire department, Designated Official, or Occupant Emergency Coordinator.</li></ul> <p><b>Other Floor Teams</b></p> <p>If floor is to be evacuated, follow Fire Floor Team instructions; if not, stand by for instructions from the Designated Official or Occupant Emergency Coordinator.</p> <p><b>Damage Control Team</b></p> <p>Follow instructions from Damage Control Team Coordinator.</p> <p>Activate, as appropriate, alarm systems, smoke control, fire extinguishers, and emergency power.</p> <p>Assist fire department and other emergency response personnel.</p> <p><b>Building occupants</b></p> <p>Evacuate the building in a calm and orderly manner using the prescribed evacuation routes and assemble with other occupants in the designated assembly area.</p> <p>Remain in the assembly area until the fire department and Designated Official have made an all-clear announcement.</p> |
|---|

### **Appendix B. Evacuation Routes**

Appendix B of the OEP should show a map of the evacuation routes from each floor of the building, preferably color-coded. Also, this information should be prominently posted on office bulletin boards and in the vicinity of elevator lobbies and stairwells.

### **Appendix C. Evacuation Assembly Area(s)**

Appendix C of the OEP should present a map showing the location of the prescribed evacuation assembly area(s), with directions on how to get there from building exits. This information should also be prominently posted on office bulletin boards and in the vicinity of building entrances/exits.

### **Appendix D. Recommended Personal Emergency Kit**

A shelter-in-place situation is expected to last only a few hours. However, in anticipation that this condition might persist for an extended period of time, occupants should consider having a personal emergency kit containing items that would alleviate discomfort (see Figure C-5).

**Figure C-5. Contents of Recommended Personal Emergency Kit**

**Contents of Recommended Personal Emergency Kit**

- A small tote bag, fanny pack, backpack, or soft-sided briefcase to hold the contents of the kit.
- At least one gallon of bottled water or more if you are on medications that require water.
- Non-perishable foil-wrapped food such as snacks and high protein bars, canned meats and canned fruits that are light and easy to carry.
- Three-day supply of prescription medications.
- Personal toiletries, including a toothbrush, toothpaste, hand sanitizers or wipes, eye drops, toilet tissue, feminine supplies etc.
- A pen and small notebook with phone numbers and e-mail addresses of family members, friends, and neighbors.
- Small first aid kit.
- Small flashlight with extra batteries.
- Battery-powered radio with extra batteries.
- Emergency “space” blanket (mylar).
- Non-electric can opener.
- Cellular telephone.

# **Department of Housing and Urban Development**

## **Physical Security Handbook for HUD Regional and Field Offices**

### **Appendix D - Contract Security Force Standards**

#### **D.1 General**

This Appendix summarizes the performance requirements, personnel qualifications, and other standards that must be met by a private company engaged to provide security force support for a HUD Regional or Field Office. Such a security force, if warranted, serves as an integral part of the comprehensive physical security program for a facility. A key determinant of whether a contract security force is required at a HUD Regional or Field Office is the Federal Security Level of the office (as discussed in Chapter 2 of this Handbook), as well as any unique environmental or threat conditions in the vicinity of a given Regional or Field Office. In most federal buildings, the Federal Protective Service (FPS) provides the security force, if required, or the General Services Administration (GSA) contracts with a private company for security force services. The information in this Appendix is applicable only for HUD-administered contracts for private non-federal security force services in space occupied and/or leased by HUD field activities. For HUD space for which GSA provides the security force, the Regional and Field Office Security Coordinators should coordinate with GSA to ensure that their contracts are implemented satisfactorily with respect to the HUD space.

Each of the standards specified in this Appendix must be addressed in all contracts for security force services. However, certain elements may be modified to reflect differing physical security requirements based on office size, location, and special circumstances. The Office of Field Administrative Resources (OFAR), in consultation and coordination with the Regional Director or Field Office Director, is responsible for: (1) developing and issuing the Request for Proposal (RFP); (2) selecting the contractor; and (3) executing and managing a contract that meets the basic standards outlined in this Appendix. Prior to making any significant modifications or changes to these standards for a given Regional or Field Office, the OFAR Director should first consult with the Director of the Physical Security Division, Headquarters Office of Security and Emergency Planning (OSEP), indicating the need for a specific modification or change.

#### **D.2 Security Force Contract Provisions**

Following a decision to issue a RFP and execute a contract for private sector security services for a designated HUD Regional or Field Office, the OFAR Director or his/her designee should: (1) advise the Director, Physical Security Division, OSEP, of the decision; and (2) adhere to the provisions of the Non-Federal Security Force Contract Guide (distributed separately by OSEP) that is the basis for the standards presented in this Appendix and provides other relevant information that should be included in a contract with the private sector for security force services.

The following pages outline the provisions and specifications that must be included in each contract for private sector security force services at a HUD Regional or Field Office.

##### **1. Scope of Work**

- Maintain security integrity by controlling access to the HUD property
- Detect and deter security breaches

- Respond to security, safety, and medical emergencies
- Enforce relevant rules and regulations

## **2. Performance Requirements (typical)**

- Protect and safeguard personnel and property
- Operate line scan and X-ray system and magnetometers, as applicable
- Provide fixed guard posts and roving patrols
- Enforce building rules and regulations
- Perform traffic control; monitor parking lots, garage, and loading dock areas
- Control issuance, storage, and retrieval of keys
- Monitor security and fire systems
- Report hazardous conditions
- Provide injury and illness assistance
- Prepare incident reports
- Take immediate action in responding to emergencies
- Provide lost and found services
- Daily procedures and maintenance re: display of the flag of the United States, as applicable

## **3. Contract Security Officer Certification**

- Meet and comply with the FPS Contract Guard Certification requirements

## **4. Personnel Qualifications and Requirements**

- Must be a United States citizen
- No felony or misdemeanor convictions
- Stable employment history
- Superior references
- Ability to perform well under stress
- Ability to deal tactfully with the public
- Strong written and verbal communication skills
- Work with minimum supervision
- Ability to follow written and verbal instructions
- Preferably a graduate of an accredited law enforcement academy or have previous military experience related to security and/or law enforcement
- Meet criteria of Department of Labor, Employment Standards Administration, Wage and Hour Division, Standard 27102

## **5. Health and Physical Proficiency Requirements**

- Physical examination documented on Standard Form 78, Certificate of Medical Examination
- In good health and not have any physical conditions that would interfere with satisfactory performance of duties in normal or emergency situations
- Free of communicable diseases and any chronic illnesses that might impair full performance of duty
- Meet vision and hearing requirements

## **6. Drug Screening**

- Pass drug screening test prior to start of work
- Annual drug screening

## **7. Age Requirements**

- Minimum age for security officers
- No maximum age, but must be fully capable of performing all duties described in contract

## **8. Project Manager/ Shift Supervisor Qualifications**

- Prescribed combination of work experience and educational credentials

## **9. Government-Furnished Equipment (GFE)**

- Varies according to type of facility and contract requirements
- Typical types of GFE include: office space; alarm and surveillance systems; hand wand metal detectors; line scan X-ray equipment and magnetometers; personal lockers for security officers; various office supplies and equipment, including telephones, fax machine, and computer(s)

## **10. Contractor-Furnished Equipment and Supplies**

- Firearms and ammunition, and safes or other secure storage for them
- Uniforms
- Supplemental equipment and supplies (e.g. flashlights, walkie-talkies, batteries, traffic control safety apparel, etc.)

## **11. Accountability for Government-Furnished Equipment**

- Periodic inventories of government-furnished equipment
- Safeguard and secure government property
- Government and contractor obligations related to the use and care of government-furnished equipment

## **12. Contractor-Furnished Security Officer Training**

- Seventy-two hours of Basic Training required for GSA certification
- Supervisory training
- Four-hour job orientation including site tour and post observation training

### **13. Contractor Furnished Supervisor Training**

- Eight hours of supervisor training, in addition to Basic Training and Firearms Training/Qualification

### **14. Firearms Training, Qualification, and Certification**

- Training that meets the relevant GSA regulations required for all security officers and supervisors
- All personnel must be qualified to carry a .38 caliber firearm, and must have their credentials in their possession at all times on duty
- All contract personnel must renew their Firearms Certification annually

### **15. Government Provided Special Training**

- Where applicable, HUD will arrange for eight hours of GSA line scan and magnetometer training for contract employees

### **16. Reporting Requirements**

- Contractor must provide incident report to HUD management within 24 hours of the occurrence
- Prepare special reports as requested

### **17. Work Schedule**

- Work schedule must provide for security services 24 hours a day, 7 days a week
- Copy of the work schedule and/or changes for all security force personnel shall be provided to HUD management at least 72 hours prior to the start of the scheduled work period

# Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Appendix E - Physical Security Status Checklist

A five-part checklist that may be used for periodic evaluation of the security posture of a HUD Regional or Field Office is presented on the following pages. This checklist is a replication of the minimum physical security standards specified for HUD field activities (see Chapter 2 of the basic Handbook).

Parts 1 through 4 address key aspects of:

**Part 1. Perimeter Security;**

**Part 2. Entry Security;**

**Part 3. Interior Security; and**

**Part 4. Security Planning and Coordination.**

Each checklist contains a number of statements addressing configuration, procedures, systems, or equipment that apply or may apply to various aspects of facility or office security. For each statement, the individual filling out the checklist should place an “x” in one of the following four columns to the right of the statement:

|                         |  |
|-------------------------|--|
| Yes                     | The statement is true and accurate.  |
| No (not necessary)      | The statement is not true because the configuration, procedure, system, or item of equipment noted is not considered necessary.  |
| No (should be required) | The statement is not true, but the configuration, procedure, system, or item of equipment is considered necessary to ensure the security of the office.                        |
| Not applicable          | Based on the federal security level, office location, or other reason, the configuration, procedure, system, or item of equipment does not apply for this particular facility. |

For any statement for which the response is other than “yes,” an explanation should be provided in the “comments” space at the bottom of the checklist. In addition, if any “yes” response needs to be amplified or explained, an appropriate comment should be made.

**Part 5, Security Checklist Narrative**, provides space to add any comments other than those entered earlier and to highlight major problems or concerns.

The final portion of Part 5 is an overall assessment of the security posture of the office. As indicated, a reason(s) must be provided for a “fair” or “poor” assessment.

## Part 1. Perimeter Security Checklist

| Description   | Yes | No<br>(not<br>necessary) | No<br>(should be<br>required) | Not<br>applicable |
|---|-----|--------------------------|-------------------------------|-------------------|
| <b><i>Parking</i></b>   |     |                          |                               |                   |
| Access to facility parking is limited to government or other designated personnel and vehicles, and to authorized visitors                            |     |                          |                               |                   |
| Access controls to adjacent parking areas are in place to minimize threats to the facility and employee exposure to criminal activity                 |     |                          |                               |                   |
| Signs are posted to alert the public to parking restrictions, and arrangements have been made for towing unauthorized vehicles                        |     |                          |                               |                   |
| A system and procedures are in place for identifying authorized vehicles and corresponding parking spaces (through placards, decals, card keys, etc.) |     |                          |                               |                   |
| Adequate lighting is provided in parking areas to ensure the safety of employees and authorized visitors, and deter illegal or threatening activities |     |                          |                               |                   |
| <b><i>Closed Circuit Television (CCTV) Monitoring</i></b>   |     |                          |                               |                   |
| Twenty-four hour CCTV surveillance cameras with time lapse video recording are used for monitoring exterior areas                                     |     |                          |                               |                   |
| Signs are posted advising of 24-hour video surveillance   |     |                          |                               |                   |
| <b><i>Exterior Lighting</i></b>   |     |                          |                               |                   |
| Lighting with emergency back-up power is provided along the building exterior and at entrances and exits  |     |                          |                               |                   |
| <b><i>Windows</i></b>   |     |                          |                               |                   |
| Shatter resistant material has been applied to all exterior windows   |     |                          |                               |                   |
| <b><i>Physical Barriers</i></b>   |     |                          |                               |                   |
| Physical barriers (concrete and/or steel composition) are in place along the perimeter of the facility  |     |                          |                               |                   |
| Parking barriers are in place to prevent unauthorized vehicle access  |     |                          |                               |                   |

**Comments:**

## Part 2. Entry Security Checklist

| Description   | Yes | No<br>(not<br>necessary) | No<br>(should be<br>required) | Not<br>applicable |
|---|-----|--------------------------|-------------------------------|-------------------|
| <b><i>Access Control</i></b>  |     |                          |                               |                   |
| Security officer is posted at entrance(s) to control building access and/or access to HUD office space  |     |                          |                               |                   |
| An intrusion detection system (IDS) with central monitoring capability is installed at the building exterior  |     |                          |                               |                   |
| Entry control is accomplished through installation of an automatic locking/remote unlocking mechanism on the entrance door(s) to HUD office space   |     |                          |                               |                   |
| An internal IDS is installed to preclude unauthorized entry into specified sensitive areas  |     |                          |                               |                   |
| Life safety standards per GSA design standards (fire detection, fire suppression systems, etc.) are installed and operable  |     |                          |                               |                   |
| <b><i>Entrances/Exits</i></b>   |     |                          |                               |                   |
| X-ray equipment and magnetometers are installed at public entrances to the facility   |     |                          |                               |                   |
| All mail/packages hand-carried into the building are subject to screening by x-ray machines and/or visual inspection  |     |                          |                               |                   |
| A glass door(s) is installed at the main entrance to HUD office space that permits visibility from within of the immediate area outside of the entrance   |     |                          |                               |                   |
| HUD office space has two ways of egress, a front door and a back door. Preferably, the doors will not be located near each other and will open out into different hallways.                         |     |                          |                               |                   |
| All exterior entrances/exits have high security locks that meet GSA specifications  |     |                          |                               |                   |
| <b><i>Receiving/Shipping Areas</i></b>  |     |                          |                               |                   |
| Package entry and access to receiving/shipping areas is controlled  |     |                          |                               |                   |
| <b><i>Posting of Government Rules and Regulations</i></b>   |     |                          |                               |                   |
| Federal government rules and regulations are posted at the entrance(s) to HUD-occupied space relative to policies such as prohibiting the unauthorized possession of firearms and dangerous weapons |     |                          |                               |                   |

**Comments:**

### Part 3. Interior Security Checklist

| Description  | Yes | No<br>(not<br>necessary) | No<br>(should be<br>required) | Not<br>applicable |
|--|-----|--------------------------|-------------------------------|-------------------|
| <b><i>Receptionist Area/Duress Alarm</i></b>   |     |                          |                               |                   |
| A receptionist area is established facing the main entrance to HUD office space  |     |                          |                               |                   |
| The receptionist area is clearly visible from the interior of the office   |     |                          |                               |                   |
| The receptionist area has a hidden duress alarm that can be unobtrusively activated by the receptionist or other employee                                  |     |                          |                               |                   |
| The duress alarm annunciates at a monitoring station that is continuously staffed  |     |                          |                               |                   |
| Access to interior office space from the receptionist area is controlled by installation of card access mechanisms or cipher locks on doors leading inside |     |                          |                               |                   |
| <b><i>Employee/Visitor Identification/Control</i></b>  |     |                          |                               |                   |
| All employees are issued a photo ID, which must be displayed at all times while in the HUD office  |     |                          |                               |                   |
| All visitors sign in and out with a receptionist or security officer   |     |                          |                               |                   |
| All visitors are screened and issued a visitor ID badge, which must be displayed at all times while in the HUD office                                      |     |                          |                               |                   |
| All visitors are accompanied by an escort while in the HUD office  |     |                          |                               |                   |
| <b><i>Mail and Package Handling</i></b>  |     |                          |                               |                   |
| The mail and package handling and sorting area is isolated from other internal activities within the HUD office  |     |                          |                               |                   |
| Access to the mail and package handling area is restricted only to designated personnel  |     |                          |                               |                   |
| Personnel assigned to mail and package handling and sorting duties have been provided security training  |     |                          |                               |                   |
| Use of rubber gloves is mandatory for all personnel handling incoming mail and packages  |     |                          |                               |                   |
| Procedures have been established for handling suspicious mail and packages, including provision of a repository for disposition of suspicious items        |     |                          |                               |                   |
| <b><i>Access to Sensitive Records and Equipment</i></b>  |     |                          |                               |                   |
| The configuration and layout of the office precludes casual/unauthorized access to sensitive records   |     |                          |                               |                   |
| Access to computer workstations and printers, copiers, FAX machines, etc., is restricted to authorized users   |     |                          |                               |                   |
| Access to telephone switching equipment is restricted to authorized users  |     |                          |                               |                   |

**Part 3. Interior Security Checklist (continued)**

| Description   | Yes | No<br>(not<br>necessary) | No<br>(should be<br>required) | Not<br>applicable |
|---|-----|--------------------------|-------------------------------|-------------------|
| <b><i>Public Address System</i></b>   |     |                          |                               |                   |
| A public address system has been installed to permit emergency announcements to all occupants of HUD office space and/or the building in which the HUD office is located  |     |                          |                               |                   |
| <b><i>Access to Public Restrooms</i></b>  |     |                          |                               |                   |
| Provisions have been made to restrict access to public restrooms to authorized personnel only   |     |                          |                               |                   |
| <b><i>Utilities</i></b>   |     |                          |                               |                   |
| Utility areas in the facility in which the HUD office is located are secure and only authorized personnel can gain entry  |     |                          |                               |                   |
| Emergency back-up power to critical systems (e.g., alarm systems, radio communications, computer facilities, etc.) is available   |     |                          |                               |                   |
| Emergency lighting is provided throughout HUD office space, including illuminated exit signs powered by the emergency lighting system.  |     |                          |                               |                   |
| A fire detection and suppression (sprinkler) system is installed that provides 100 percent coverage of HUD office space.  |     |                          |                               |                   |
| <b><i>Protection from airborne chemical, biological, or radiological (CBR) attack</i></b>   |     |                          |                               |                   |
| Access to fresh air intakes, mechanical areas, and roof tops in the facility in which the HUD office is located is strictly controlled  |     |                          |                               |                   |
| Access to building heating, ventilation, and air conditioning (HVAC) systems information is restricted to authorized personnel only   |     |                          |                               |                   |
| Procedures are in place for notification of the building manager, security force desk, local emergency personnel, and/or other key personnel in the event that toxic airborne hazards are suspected or detected |     |                          |                               |                   |

**Comments:**

### Part 4. Security Planning and Coordination Checklist

| Description   | Yes | No<br>(not<br>necessary) | No<br>(should be<br>required) | Not<br>applicable |
|---|-----|--------------------------|-------------------------------|-------------------|
| <b><i>Physical Security Plan</i></b>  |     |                          |                               |                   |
| A comprehensive Physical Security Plan for the HUD office exists and is kept current  |     |                          |                               |                   |
| Copies of the Physical Security Plan are made available to all office employees   |     |                          |                               |                   |
| Provisions of the Physical Security Plan are made known to all employees through a comprehensive security training, education, and awareness program  |     |                          |                               |                   |
| <b><i>Occupant Emergency Program</i></b>  |     |                          |                               |                   |
| An Occupant Emergency Organization (OEO) has been established and includes the participation of all tenants in the facility in which the HUD office is located  |     |                          |                               |                   |
| An Occupant Emergency Plan (OEP) is in place, updated annually, and periodically tested   |     |                          |                               |                   |
| Copies of the OEP are made available to all office employees  |     |                          |                               |                   |
| A formal OEP test, training, and exercise program has been established  |     |                          |                               |                   |
| <b><i>Standardized Alert Levels and Threat Conditions</i></b>   |     |                          |                               |                   |
| Standardized alert levels and threat terminology have been established  |     |                          |                               |                   |
| Procedures are in place to disseminate alert level and threat information to all concerned in a timely manner   |     |                          |                               |                   |
| Provisions have been made to jointly upgrade alert levels and security procedures in the facility in which the HUD office is located during emergency situations such as terrorist attacks, natural disasters, and/or civil unrest  |     |                          |                               |                   |
| <b><i>Security Training, Education, and Awareness</i></b>   |     |                          |                               |                   |
| Security training and awareness materials have been developed and distributed, as appropriate, to provide up-to-date information covering security practices, employee security awareness, personal safety during emergencies, etc. |     |                          |                               |                   |
| A formal security training program has been established, including a new employee orientation and an annual update for all HUD employees  |     |                          |                               |                   |
| <b><i>Background Security Checks for Contract Service Personnel</i></b>   |     |                          |                               |                   |
| Background security checks and security control procedures are required for contract service personnel within the facility in which the HUD office is located   |     |                          |                               |                   |

**Comments:**

## Part 5. Security Checklist Narrative

**Other comments concerning office security not covered above:**

**Major problems or concerns:**

**Overall assessment of security posture:**

\_\_\_ **Excellent**      \_\_\_ **Good**      \_\_\_ **Fair**      \_\_\_ **Poor**

**If assessment is fair or poor, indicate reason(s) below.**

**Approved:**

# Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Appendix F - Field Office Physical Security Status Report

An annual **Physical Security Status Report** (Report) will be prepared by each HUD Field Office and submitted to the Security Coordinator of the Regional Office under which the Field Office is located. The Report will contain two parts:

- **Part I** of the Report will be prepared by the Field Office Security Coordinator and approved by the Field Office Director. It will include an overall assessment of the security posture of the Field Office, including recommended corrective actions, based on a comprehensive survey using the checklist described in Appendix E; and
- **Part II** of the Report will provide an opportunity for the Regional Office to comment on the information included in Part I and present any additional information that may be pertinent to the security status of the Field Office.

Part I of the Report will be submitted by each Field Office to its Regional Office by October 15 of each year and will cover the period October 1 through September 30 of the preceding fiscal year. The Regional Office will complete Part II of each Field Office Report and incorporate all Reports into a consolidated Regional Summary Report (see Appendix G) for subsequent distribution to: the Director, Physical Security Division, Office of Security and Emergency Planning (OSEP), Headquarters, HUD, and the HUD Headquarters Office of Field Policy and Management (FPM).

Completed Field Office Security Status Reports are an important source of background information and justification for funding any improvements in the security posture of each office. In addition, information provided in any of the Reports may engender a follow-up visit(s) by a Headquarters Quality Management Review (QMR) team or other outside entity to validate the information provided in the Report.

A suggested organization and format for the Field Office Physical Security Status Report are shown in Figure F-1 on the following two pages.



**Figure F-1. Format – Field Office Physical Security Status Report (continued)**

|   |
|---|
| <p style="text-align: center;">_____ <b>Field Office Physical Security Status Report</b><br/><b>for period October 1, 20xx, through September 30, 20xx</b></p> <p style="text-align: center;"><b>Part II. Regional Comments</b></p> <p><b>1. (Concur) (Do not concur) in overall assessment of security posture.</b><br/><b>Reason(s) for non-concurrence, if applicable:</b></p> <p><b>2. (Agree) (Do not agree) with recommended corrective actions and order of priority.</b><br/><b>Reason(s) for non-agreement, if applicable:</b></p> <p><b>3. Additional comments and/or suggestions.</b></p> <p style="text-align: right;">_____<br/><b>Regional Office Security Coordinator</b></p> <p style="text-align: right;">_____<br/><b>Regional Director</b></p> |
|---|

# Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Appendix G. Regional Physical Security Status Report

An annual, consolidated **Regional Physical Security Status Report** will be prepared by each HUD region and will consist of a **Summary Report** (see outline of contents in Figure G-1) with:

**Enclosure 1.** The **Regional Office Physical Security Status Report** (see organization and format in Figure G-2); and

**Enclosures 2 through x.** The **Field Office Physical Security Status Reports** for each Field Office in the Region (as described in Appendix F).

The Regional Office Physical Security Status Report (Figure G-2) will focus only on the Regional Office itself and will contain the same information as Part I of a Field Office Physical Security Status Report.

The Regional Summary Report will summarize highlights from the Regional Office Physical Security Status Report and the individual Field Office Physical Security Status Reports. In general, the Summary Report should address areas of concern, security issues, lessons learned, etc. from a Region-wide perspective focusing on matters that are applicable across-the-board. However, in the instance that a truly egregious security problem or issue exists at only one or a few HUD facilities in the Region, that should be duly noted in the Summary Report as a matter requiring priority attention.

The Summary Report, with the enclosures as indicated, should be submitted by October 31 of each year to the Director, Physical Security Division, Office of Security and Emergency Planning (OSEP), Headquarters, HUD, and the HUD Headquarters Office of Field Policy and Management (FPM).

**Figure G-1. Outline – Regional Physical Security Status Summary Report**

**Physical Security Status  
for period October 1, 20xx, through September 30, 20xx  
Region \_\_\_\_\_  
Summary Report**

\_\_\_\_\_  
(date)

- 1. Security-related incidents during reporting period, including action(s) taken.**
- 2. Security reviews, including results, conducted during reporting period.**
- 3. Prevailing areas of concern and/or most pressing security issues.**
- 4. Lessons learned.**
- 5. Region-wide security-related initiatives undertaken during reporting period.**
- 6. Sufficiency of funding for security-related projects.**
- 7. Overall assessment of security posture.**
- 8. Recommendations for enhancing security in order of priority.**

\_\_\_\_\_  
**Regional Director**

**Enclosures: Regional Office and Field Office Physical Security Status Reports**

**Figure G-2. Format – Regional Office Physical Security Status Report**

|   |                                 |
|---|---------------------------------|
| <b>Regional Office Physical Security Status Report</b><br><b>for period October 1, 20xx, through September 30, 20xx</b> |                                 |
|   | _____<br>(date)                 |
| <b>Region:</b> _____  |                                 |
| <b>Leased or Federal:</b> _____   | <b>Office Population:</b> _____ |
| <b>Federal Security Level:</b> _____  |                                 |
| <b>1. Date of Office <i>Physical Security Plan</i>:</b>   |                                 |
| c. Website location:  |                                 |
| d. Type and dates of security education, training, and awareness activities conducted during the year:                  |                                 |
| <b>2. Date of Office <i>Occupant Emergency Plan (OEP)</i>:</b>  |                                 |
| c. Website location:  |                                 |
| d. Type and dates of OEP drills, training activities, and exercises conducted during the year:                          |                                 |
| <b>3. Security-related incidents during reporting period, including action(s) taken:</b>                                |                                 |
| <b>4. Other problems or areas of concern:</b>   |                                 |
| <b>5. Overall assessment of security posture:</b>   |                                 |
| <b>6. Recommended corrective actions in order of priority:</b>  |                                 |
| <b>Survey conducted by:</b> _____<br><b>Regional Office Security Coordinator</b>  |                                 |
| <b>Approved:</b> _____<br><b>Regional Director</b>  |                                 |

# Department of Housing and Urban Development

## Physical Security Handbook for HUD Regional and Field Offices

### Appendix H - Urgent Physical Security Issue Report

An urgent physical security issue(s) requiring immediate attention may arise in any HUD Regional or Field Office at any time. Such an issue may involve physical damage to the facility, a situation that creates a hazardous environment for occupants of the office, or some other condition that has an adverse effect on the security of office operations.

In such cases, a telephonic report should be made immediately, followed up by e-mail as soon as practicable to:

- The Regional Director (for Field Offices);
- The Director of the Office of Field Administrative Resources (OFAR);
- The HUD Headquarters office of Field Policy and Management (FPM); and
- The Director, Physical Security Division, Office of Security and Emergency Planning (OSEP), HUD Headquarters.

The information to be provided in the report is indicated in Figure I-1.

#### Figure H-1. Contents of Urgent Physical Security Issue Report

|  |
|--|
| <p><b>From:</b></p> <p><b>To:</b></p> <p><b>Subject: Urgent Physical Security Issue</b></p> <ol style="list-style-type: none"><li>1. Briefly describe the nature of the urgent physical security issue and the impact on personnel, property, and/or office operations. If the issue was caused by a specific incident or incidents, provide the time/date of the incident(s).</li><li>2. Indicate actions taken locally in dealing with the issue and the results. If applicable, identify any agencies outside of HUD that are or have been involved (e.g., GSA, FPS, FBI, local law enforcement, local fire department, etc.).</li><li>3. Indicate corrective action(s) deemed necessary to rectify the situation and resolve the issue.</li><li>4. Describe the consequences if this issue is not dealt with in a timely manner.</li><li>5. State whether or not the issue has been separately reported as an incident under the HUD Incident Management System (HIMS) or other communication; and cite the specific prior report or other communication if applicable.</li><li>6. Provide any additional comments and/or recommendations.</li></ol> |
|--|

**Department of Housing and Urban Development**  
**Physical Security Handbook for HUD Regional and Field Offices**

**Appendix I. Glossary of Acronyms and Terms**

**I.1 Acronyms**

|        |   |
|--------|---|
| AO     | Administrative Officer  |
| BM     | Building Manager  |
| CBR    | Chemical, Biological, or Radiological                                     |
| CCTV   | Closed Circuit Television   |
| CIA    | Central Intelligence Agency   |
| COOP   | Continuity of Operations  |
| CPR    | Cardiopulmonary Resuscitation   |
| DCT    | Damage Control Team   |
| DCTC   | Damage Control Team Coordinator   |
| DOD    | Department of Defense   |
| DHS    | Department of Homeland Security   |
| DO     | Designated Official   |
| DOJ    | Department of Justice   |
| ECC    | Emergency Command Center  |
| ECCT   | Emergency Command Center Team   |
| FBI    | Federal Bureau of Investigation   |
| FM     | Floor Monitor   |
| FPM    | Office of Field Policy and Management                                     |
| FPS    | Federal Protective Service  |
| FT     | Floor Team  |
| FTC    | Floor Team Coordinator  |
| FOD    | Field Office Director   |
| GAO    | Government Accountability Office (formerly the General Accounting Office) |
| GSA    | General Services Administration   |
| GFE    | Government Furnished Equipment  |
| HAZMAT | Hazardous Materials   |
| HSAS   | Homeland Security Advisory System   |
| HUD    | Department of Housing and Urban Development                               |
| HVAC   | Heating, Ventilation, and Air Conditioning                                |
| HIMS   | HUD Incident Management System  |
| ID     | Identification [badge or system]  |
| IDS    | Intrusion Detection System  |
| ISC    | Interagency Security Committee  |
| MC     | Medical Coordinator   |

|      |   |
|------|---|
| OAMS | Office of Administrative and Management Services (Office of Administration) |
| OBAS | Office of Budget and Administrative Support (Office of Administration)      |
| OEC  | Occupant Emergency Coordinator  |
| OEO  | Occupant Emergency Organization   |
| OEP  | Occupant Emergency Plan   |
| OFAR | Office of Field Administrative Resources (Office of Administration)         |
| OSEP | Office of Security and Emergency Planning (Office of Administration)        |
| PSAG | Physical Security Advisory Group  |
| PSS  | Physical Security Specialist  |
| QMR  | Quality Management Review   |
| RD   | Regional Director   |
| SDB  | Space Design Branch (OAMS)  |
| TT&E | Test, Training, and Exercises   |
| UPS  | Uninterrupted Power Supply  |

## I.2 Terms

**Access Control.** An aspect of physical security that utilizes hardware systems and/or specialized procedures to control and monitor the movement of individuals, materials, or vehicles into, out of, or within designated areas.

**Access Control System.** A combination of electronic, electro-mechanical, mechanical, or physical means configured to identify authorized personnel and admit them into a designated area.

**Closed Circuit Television (CCTV).** A television system, usually hard-wired, used for observation and surveillance of designated areas within a facility or office.

**Controlled Access Area.** A specifically designated area, such as a room or office where sensitive or privileged information has been authorized for handling, storage, discussion, or processing, and for which supplemental controls have been established to monitor, control, or limit access only to authorized personnel.

**Designated Official (DO).** The individual who is the highest-ranking federal official in a given facility (or other person agreed upon by all tenant agencies). The DO directs the activities of the local OEO in implementation of the OEP.

**Duress Alarm.** A hidden alarm that can be unobtrusively activated by a receptionist or other individual to warn of a threatening situation.

**Entry Security.** The application of security standards for the protection of occupants and imposition of controls relative to the entry of persons, equipment, and packages into a given facility.

**Facility.** A physical building, structure, or complex in which a HUD Regional or Field Office is located.

**Federal Facility.** A facility that is owned or under the management and control of the Federal Government.

**Federal Security Levels.** Five security levels (I, II, III, IV, and V) established to determine minimum security standards for each level based on factors such as size of a given facility, number of employees, primary activity, the need for public access, and other factors such as perceived threat, crime statistics in the local area, etc.

**Homeland Security Advisory System (HSAS).** A set of graduated threat conditions used to alert federal departments and agencies to implement specified protective measures in order to minimize vulnerability to terrorist attacks. From lowest to highest, the threat conditions are identified by color as: (1) green – low risk; (2) blue – guarded risk; (3) yellow – elevated risk; (4) orange – high risk; and (5) red – severe risk.

**Information Security.** The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.

**Interagency Security Committee (ISC).** A permanent body established by Executive Order 12977 that is chaired by GSA and consists of representatives from the federal cabinet-level departments and other federal agencies. The principal responsibilities of the ISC are to: establish policies for the security and protection of federal facilities; develop and evaluate security standards for federal facilities; and develop a strategy for ensuring compliance with such standards.

**Interior Security.** The application of security standards for the protection and safeguarding of employees, information, equipment, and materials within a given facility against espionage, sabotage, damage, theft, and/or unauthorized access.

**Intrusion Detection System (IDS).** A system designed to detect and monitor unauthorized entry or attempted entry into a facility or designated area.

**Leased Space Facility.** A facility that has been leased by the Federal Government for conducting government business and the level of security that is attainable in a federal facility may not be possible.

**Monitor.** (1) A video display unit used with a CCTV system. (2) A centrally-located alarm processing device that receives alarm signals and displays system status.

**Occupant Emergency Organization (OEO).** A group of employees assigned to undertake certain responsibilities and perform specific tasks in response to an emergency that threatens a facility and/or its occupants.

**Occupant Emergency Plan (OEP).** A document that delineates a set of procedures designed to protect life and property in federally-occupied space under specified emergency conditions.

**Perimeter Security.** Application of security standards for the protection and safeguarding of personnel, vehicles, and equipment in the external areas of a given facility, which may include the outside walls of a building, sidewalks, parking areas, and adjoining areas.

**Physical Security.** That part of security concerned with physical measures to: provide for the individual and collective safety and well-being of personnel; prevent unauthorized access to a designated facility; and safeguard information, equipment, materials, and documents within the facility against espionage, sabotage, damage, theft, and/or unauthorized disclosure.

**Physical Security Advisory Group (PSAG).** An internal group within HUD, chaired by the Director, Physical Security Division, OSEP, established to oversee, review, coordinate, and make recommendations on the processes and procedures employed to ensure the physical security of each HUD Regional and Field Office.

**Physical Security Plan.** A document that delineates the procedures to be followed and systems and equipment employed to ensure the safety and protection of the personnel, information, equipment, and materials located in a given facility and to preclude unauthorized access into the facility.

**Physical Security Specialist.** A trained individual whose primary duties include analytical, planning, advisory, operational, or evaluative work that has as its principal purpose the development and implementation of policies, procedures, standards, training, and methods for safeguarding and protecting information, personnel, property, facilities, operations, or materials from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss.

**Security Assessment.** A report containing a fundamental evaluation and analysis of security-related devices, equipment, services, and procedures in use at a given location, including development of recommendations for security improvements or enhancements.

**Security Coordinator.** An individual designated by a HUD Regional or Field Office Director as the principal point-of-contact on all matters relating to ensuring the security of the office, including development and coordination of all aspects of implementation and testing of a local OEP and Physical Security Plan.

**Security Standards.** Standards applied to each Federal Security Level for ensuring the proper protection and safeguarding of personnel and property relative to security planning and to the perimeter, entry, and interior security of federal facilities, whether leased or government-owned.

**Security System.** A term applied to the totality of a facility's security equipment, processes, and procedures (e.g., locks, surveillance equipment, access controls, alarms, security officers, etc).

**Surveillance.** Involves the observation or inspection of persons or premises for security purposes through alarm systems, CCTV, visual scrutiny, and/or other means.