Federal Real Property Council
Security Resource Guide

Spring 2003

A Guide to Federal Security

Office of Real Property

Overview

The Federal Real Property Council (FRPC) is a group of senior level real property executives from more than 30 Federal agencies representing the global portfolio of all Federal real property assets. The Council provides a forum to address critical real estate and workplace issues challenging all Federal agencies. The FPRC is currently co-chaired by David Bibb, Deputy Associate Administrator, Office of Real Property, General Services Administration, and has been co-chaired by Gary Arnold, Deputy Associate Commissioner, Office of Facilities Management, Social Security Administration. The FPRC identified security as its number one issue to address in 2002

and formed a work group of representatives from a cross section of Federal agencies, including the Departments of Agriculture, Justice, State, and Interior, as well as NASA, National Research Council, OPM, SBA, SSA and GSA. The work group was chaired by Gary Arnold (SSA), and facilitated by Marjorie Lomax (GSA), and Andrea Wohlfeld Kuhn (GSA).

The work group began in March 2002 and quickly acknowledged that there was sufficient policy available or being created in other arenas and that its focus would be on how best to function in the day-to-day environment facing each agency. That led the group to concentrate on four major security areas:

Gary Arnold
(SSA), Work Group Chair

Through a series of meetings and featured speakers, the group acknowledged the need for improvement and, at the same time, identified the outstanding practices to be found in each agency. Many of the ideas and practices are simple measures that may appear obvious, but they are all worth repeating. Among the group members, each participant found many actions that would enhance their security pro-grams, frequently with minimal effort and expense. In the hope that others will find these ideas and practices equally useful, the work group offers this *Security Resouce Guide*. ∎

I. Design and Construction

This section identifies the relevant policies, guidelines and standards affecting security and construction and alteration projects in leased and Federally owned buildings. Secondly, a synopsis of currently available information and general guidelines of resources is provided to assist agencies in incorporating appropriate levels of security into their facilities. Relevant web sites are found at the end of the document.

The security needs of each agency and building are dependent on the threats to the agency and physical characteristics of the building. Security guidelines should be on a case-by-case basis and should be tailored to address the specific threat and vulnerability. In general, agencies should look for and follow the recommendations of the Interagency Security Committee (ISC), which is responsible for publishing guidelines for security improvements at both leased and owned buildings.

Applicable Security Standards and References

- DOD Antiterrorism Minimum Construction Standards for Buildings http://www.tisp.org/files/pdf/dodstandards.pdf

- GSA Facilities Standards for the Public Buildings Service (Section 8 and others) http://hydra.gsa.gov/pbs/pc/facilitiesstandards/

- DOJ Vulnerability Assessment of Federal Facilities (contact Adam Bodner at Adam.H.Bodner@usdoj.gov)

- Document security for sensitive but unclassified paper and electronic building information, GSA 3490.1, March 8, 2002 at http://www.gsa.gov (search FMR)

- Mail Room Safety information available at http://www.gsa.gov and through the U.S. Department of Health and Human Services, Centers for Disease Control and Prevention at http://www.bt.cdc.gov/

- Technical Assistance Document for Anthrax Cleanup at http://www.nrt.org/production/nrt/home.nsf

- FMR 102-71 through 102-83 "Real Property Policies Update" at http://www.gsa.gov

- FPS Occupant Emergency Program Guide at http://www.gsa.gov

- Sources for execution (design and construction): GSA term contracts, MOBIS schedule, etc. at http://www.gsa.gov under Security Design and Construction

"The security needs of each agency and building are dependent on the threats to the agency and physical characteristics of the building."

I. Design and Construction

Checklist

Significant security issues to consider related to construction and alteration projects.

- Setbacks
- Progressive collapse
- Control of parking and first floor retail
- Window glazing/framing
- Electronic security/access control systems
- Biohazard mitigation
- Anthrax decontamination
- Isolated air handling for mail centers
- Back-up public utilities (emergency power)

Points of Contact

Major federal agency headquarters have projects underway in the National Capital Region, which will require the application of new security standards/criteria. The following points of contact can provide further information:

- Alcohol, Tobacco, and Firearms (ATF) Headquarters Project: Mignon Anthony, (202) 927-1688
- Patent and Trademark Office (PTO) Headquarters Project: Rick Hendricks, Project Manager, (202) 401-4319
- Pentagon Modernization/Renovation http://renovation.pentagon.mil

Questions and Answers

Who do I contact in the GSA Central Office for security surveys of my agency's buildings and office space throughout the US?

Bruce A. Davis at (202) 219-1236

What are typical security costs as a percentage of new construction and renovation/alteration projects?

Costs average 6 to 8 % for new construction while renovations and alterations costs depend on the building and are site-specific

What is GSA's schedule for conducting surveys?

Surveys are conducted of GSA's building inventory depending on the level of the facility, as defined by the June 28, 1995 Department of Justice Vulnerability Assessment of Federal Facilities:

- Level 1 (10 or fewer federal employees): Survey conducted every 4 years
- Level 2 (11-150 federal employees): Survey conducted every 4 years
- Level 3 (151-450 federal employees): Survey conducted every 3 years
- Level 4 (450 or more federal employees): Survey conducted every 2 years
- Level 5 (a facility such as the Pentagon or CIA Headquarters with missions critical to national security): Survey conducted every year ■

A. Aids for Employees

In its examination of how various departments and agencies handle physical security, the FRPC work group discovered or identified a number of aids that can make it easier for employees to keep requirements and procedures in mind. Here are several:

Wallet sized emergency procedure cards

These wallet cards can be designed to contain whatever information the agency deems most critical. For example, the card can contain, in simple abbreviated language, the steps each person must take to evacuate the building in an emergency, including where to regroup and how to report should the building be closed. They can also indicate the color or numerical emergency codes used and their meanings.
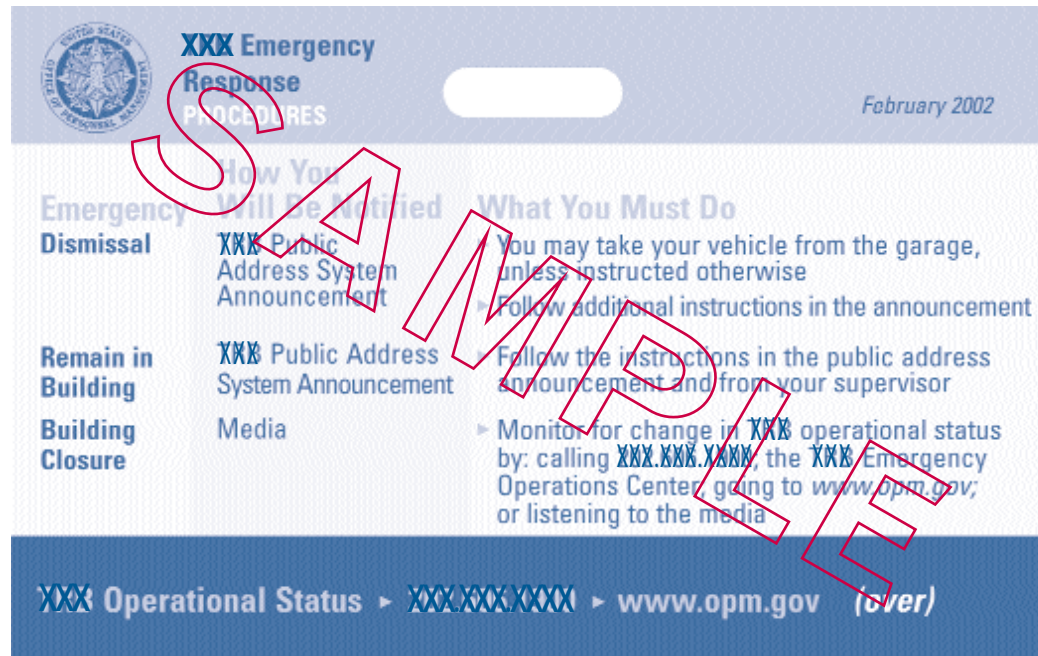
Often the cards contain emergency numbers, names of contacts, and hotline numbers for employees to report suspicious activities, emergencies and deficiencies/inconsistencies in practices and a website with frequently asked questions (FAQ) about security policy.

Several agencies have found it useful to make the cards compatible with access badges so that employees have the information with them at all times.

An example is provided by OPM (see illustration above at right).

Bomb Threat or Emergency Contact Cards

There are a number of aids that employees can keep at their workstations, near their telephones or computers that give step-by-step instructions in case of an emergency. An example is the FBI's Bomb Data Center card (FBI Form FD 730), which contains the key items the person receiving the call should elicit from the caller. Similar cards, tailored to individual agency needs (see GSA example on next page), contain agency-specific information, like emergency telephone numbers, which can be affixed to the telephone.

It is best to keep the cards simple and advisable to make them a different color than normal notices and correspondence, so that the individual can find them in a hurry. The emphasis is on enabling the person who is responding to do so as calmly and as quickly as possible, without having to rely solely on memory.

Security Reminders

Many agencies have found it valuable to reinforce security by sending out specific messages regularly with each message concentrating on an individual issue, such as reminders about how to identify and handle suspicious packages. In some cases there are posters to accompany these reminders available through another agency (e.g., the USPS poster on suspicious mail). While much information can be sent via email, sometimes to overcome the email overload many employees experience, it is good to find another venue or to use several venues simultaneously. Desk to desk distribution of a brightly colored fact sheet (and using the same color for all security related material), along with the use of in house newsletters and publications can be very effective.

Examples include:

- USPS poster

- Internal agency bulletins such as the Social Security Administration's Bulletin on Suspicious Packages

Actions for a Bomb Threat:

- Keep calm. Keep talking.
- Don't hang up.
- Signal a co-worker to get an extension.
- Ask caller to repeat the message and write it down.
- Repeat questions, if necessary.
- Ask where the bomb is and when it is set to go off.
- Listen for background noises.
- Write down noises, gender, pitch of voice and accent.
- Ask person's name, exact location, phone number.
- Signal a co-worker to call FPS, guard or local police.
- Notify your immediate supervisor.

If Faced with a Gun, Knife, or Weapon Threat:

- Stay calm. Quietly signal for help.
- Maintain eye contact.
- Stall for time.
- Keep talking -- but follow instructions from the person who has the weapon.
- Don't risk harm to yourself and others.
- Never try to grab a weapon.
- Watch for a possible chance to escape to a safe area.

Sample of GSA bomb threat/emergency card

from each of the Federal agencies occupying the building. The BSC also ensures that people follow proper security practices in the building and that employees receive training concerning the Occupant Emergency Plan and security awareness. The BSC must continually evaluate standards to make sure they protect the facility. For its inventory of buildings, GSA will normally conduct routine security assessments and then share, discuss, and validate findings with the BSC during a regular meeting. However, the BSC should meet whenever tenants or an agency's mission changes.

All agencies, and particularly those that involve face-to-face service to the public, can benefit from formally recording incidents. The collection and analysis of this information over time allows agencies to modify their security programs and justify expenditures. This information also is a solid basis for objective discussions by building security committees as they determine the appropriate security procedures and equipment for a facility. It is critical that the agencies housed in a multi-tenant facility share this information with the other occupant agencies since an incident in one office can easily affect other offices as well.

The types of incidents captured depend to some extent on the level of interaction with the public.

Agency examples include:

Communications

Most agencies depend on computers, telephones and pagers/beepers of various types to communicate during emergencies. Given the situation these may or may not work, so it is vital that there be back up systems. For example, if there is an automated

Incident Reporting

Federal Management Regulation (FMR) Section 102-74.15 requires that occupant agencies in GSA space promptly report all crimes and suspicious circumstances occurring on federally controlled property first to the regional law enforcement organization and other designated law enforcement agencies, and then through internal agency channels. In addition, GSA investigates crimes committed on property it controls

and exchanges intelligence information with other Federal, State and local law enforcement agencies.

Since security needs vary by location, even among facilities at the same security level, the Department of Justice's (DOJ) Vulnerability Assessment of Federal Facilities established the Building Security Committee (BSC) as a formal mechanism for addressing security concerns at each facility. The BSC should consist of representative(s)

II. Existing Space (Leased and Government-Owned)

sign-in system and access to the system is unavailable, it may be difficult to reconstruct who was at work on the day of the incident. Or if the communications systems are down or overloaded, at least the key emergency response personnel should have some alternative method of communicating.

Many of the newer building emergency systems provide voice instructions (e.g., there is a fire in Building A; only the occupants of Building A need vacate at this time). While these systems are appropriate and valuable, many times the announcements are misunderstood or the programmed announcements do not apply to the situation. Again there needs to be a backup or an override, and one that is tested to verify its operation. An emergency backup is an automated message that overrides whatever the activity is on an individual's computer screen at the time. Special attention needs to be paid to the requirements for persons with disabilities and to people who may be unfamiliar with the building. Section 7 of GSA's Facilities Standards for the Public Buildings Service addresses "Audible Notification Appliances" requirements, and can be accessed at http://hydra.gsa.gov/pbs/pc/facilitiesstandards/.

Agency examples include:

USDA or Pentagon message systems

- Accommodations for Persons with Disabilities

Individual arrangements need to be made for persons with disabilities and consideration must include visitors to the facility as well. There are many devices that should be evaluated, including strobe lights for the hearing impaired and special
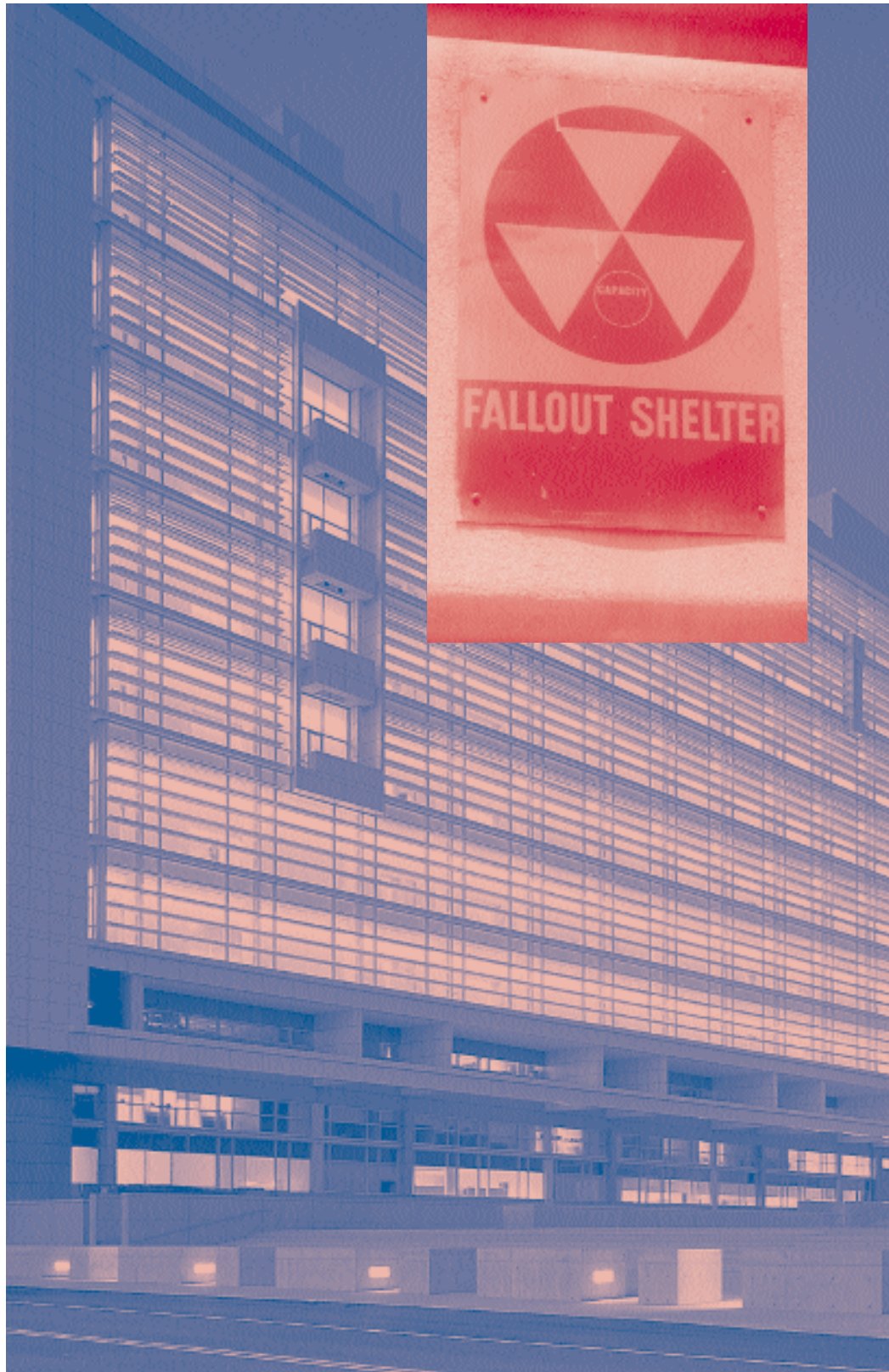
II. Existing Space (Leased and Government-Owned)

chairs for assisting mobility impaired individuals for evacuating (and which allow assistants to evacuate via stairways). Attention needs to be directed to the assignment of monitors or aides, as well as the assignment of backups or alternates. Because employees and visitors may be anywhere in the facility at the time of the emergency, additional devices should be available as well. Buses, vans, etc. may be available to shelter employees with disabilities during emergencies.

Accommodations requirements are found in 36 CFR 1190, "Minimum Guidelines and Requirements for Accessible Design," and 36 CFR 1191, entitled "Americans with Disabilities Act (ADA) Accessibility Guidelines for Buildings and Facilities." The GSA Occupant Emergency Program Guide at http://www.gsa.gov also provides guidance such as assisting handicapped persons out of the building and knowing the locations and telephone numbers of the handicapped persons to be assisted, the types of handicaps, and the location of crutches, wheelchairs, and other support devices. All devices (such as strobe lights and the special chairs for assisting mobility impaired individuals) should be evaluated in light of handicapped accessibility standards and fire and life safety standards.

An example is the evacuation chair, which can be used for stairway evacuation and emergency transport. It can be easily stored on walls in stairways or an employee's workspace.

B. Emergency Power Considerations

Section 6.11, entitled "Emergency Power Systems," of the Facilities Standards for the Public Buildings Service (PBS-P100), requires that all new GSA-constructed facilities have an emergency power system for life safety as required by code. It must be designed in accordance with NFPA 110, Emergency and Standby Power Systems. Also, the GSA leasing solicitation for offers (SFO) requires that emergency building power for life safety systems be provided in GSA-leased buildings.

In addition, the Interagency Security Committee (ISC) Security Design Criteria for New Federal Office Buildings and Major Modernization Projects provides electrical engineering criteria aimed at protecting the electrical system and ensuring that it functions in the event of a blast. During an emergency, the electrical system maintains power to essential building services, facilitates evacuation, and allows for continuing communication. These design criteria also specify the need for a tertiary power source, such as a trailer-mounted generator, for buildings where operational continuity is critical. Additionally, the ISC Security Design Criteria indicate that the electrical system should be coordinated with the building's Occupant Emergency Plan requirements. Information on design criteria is available at http://hydra.gsa.gov/pbs/pc/facilitiesstandards/.

Renovations to the Pentagon include provisions for illuminated directional arrows and signs in case of power outages and other emergency situations. More information can be found at http://renovation.pentagon.mil/. ∎

III. Occupant Emergency Organizations

Each government agency and facility in Federally owned or leased space is required to have an Occupant Emergency Plan (OEP) supported by an Occupant Emergency Organization (OEO). GSA regulations state that officials shall be designated as members of the OEO organization as well as receive training specifically tailored to their positions. The OEP should detail:

- Responsibilities
- Emergency numbers
- Primary evacuation procedures and routes
- Alternate routes
- Assembly areas
- Contact lists

The OEP's primary purpose has been to evacuate the facility in the face of fire or natural disasters. It may be supplemented, if necessary, by a Security Action Plan (SAP) which delineates procedures to follow in case of incidents involving the public, protests, terrorist threats or attacks. The important consideration is that the plan or plans address as many contingencies as possible. The focus has to be on solid preparation, followed by practice. Conducting drills under varying circumstances is the best possible measure to take.

A key factor in the OEP is the delineation of duties with the assignment of backup and support roles so that in the absence of one individual, another can step in seamlessly. This is especially important in the evacuation of persons with disabilities. As people move about the facility during the workday, they may be away from their primary location when the emergency occurs. Having additional people trained to assist in evacuations is critical to the safety of all.

Monitors may play a key role in ensuring dissemination of information and prompt evacuation in an emergency. Monitors should be easily identifiable; some agencies use brightly colored vests, armbands and/or hats to facilitate identification. In an emergency, hats may prove more visible than other items.

Another key factor is the relationship between the federal facility managers and the local fire, law enforcement and emergency response personnel. Response times can be kept to the minimum possible if everyone involved knows who to call and the respondents know how and where to respond.

Once the plan is developed and explained to facility occupants, it cannot remain static. People move in and out of offices, telephone numbers and methods of contact change, and the plans must be updated quarterly if not more frequently depending on the situation in the facility.

Several departments and agencies have been updating and expanding their OEPs and are willing to share their documents:

OPM – contact Wayne Steneck at wpstenec@opm.gov

SSA – contact Brian Clevenger at (410) 965-4542, or brian.clevenger@ssa.gov

USDA –contact Ed Campbell at (202) 720-2371 or edc.Campbell@usda.gov ■
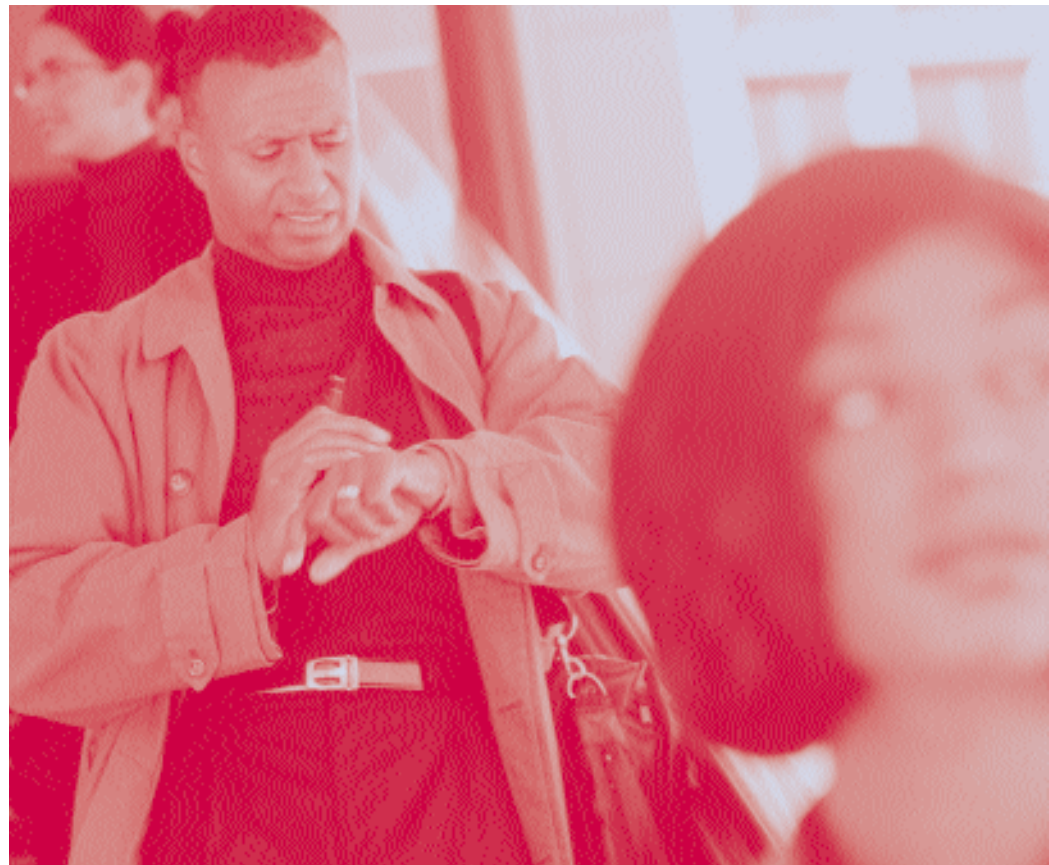
IV. Sharing Information/ Valuable Resources

Before listing sites that have valuable information, it is necessary to issue a reminder about the need to exercise extreme caution before sharing security-related information. Specifics about building layouts, exits, locked doors, etc. that are in Occupant Emergency Plans (OEP)s should not be disseminated beyond a need to know. Emergency call in numbers can be publicized, but the phone numbers for individuals should be guarded. ■

Web Sites

A. Federal Agencies and Programs

Air Force Civil Engineering Support Agency

http://www.afcesa.af.mil/

Air Force Center for Environmental Excellence (AFCEE)

http://www/afcee.brooks.af.mil/afceehome.asp

Department of Health and Human Services, Centers for Disease Control and Prevention (Information on bioterrorism, select agent regulations)

http://www.cdc.gov

Department of Homeland Security

http://www.dhs.gov

Department of State
Travel Warnings and Consular Information Sheets

http://travel.state.gov/travel_warnings.html#a

AFCEE Force Protection Handbook

http://www.afcee.brooks.af.mil/dc/dcd/arch/force.pdf

Federal Emergency Management Agency (FEMA)

http://www.fema.gov

Many publications are available, including How-To Guide #7: Integrating Human-Caused Hazards Into Mitigation Planning

http://www.fema.gov/fima/planning_toc6.shtm

General Services Administration (GSA): A variety of information is available through www.gsa.gov and then searching for the desired topic. Among others, the following may be of interest:

GSA Making Federal Buildings Safe

http://www.gsa.gov/Portal/content/pubs_content.jsp?contentOID=119420&contentType=1008

GSA Security Solutions Catalog

http://www.gsa.gov/Portal/content/pubs_content.jsp?contentOID=117096&contentType=1008

Office of Federal Protective Service

Effective March 1, 2003, the FPS was transferred to the Border and Transportation Security Directorate of the Department of Homeland Security. Until further notice, all phone numbers and points of contact contained in the GSA website at www.gsa.gov for FPS personnel nationwide and emergency and non-emergency numbers remain unchanged.

IV. Sharing Information/ Valuable Resources

GSA Mail Communications Policy (includes standards and guidelines for federal mail centers, including many related documents, such as responding to anthrax threats, mail center security management, irradiated mail, etc.)

http://www.gsa.gov/Portal/content/orgs_content.jsp ?contentOID=22920&contentType=1005

Interagency Security Council (ISC) Design Criteria

http://hydra.gsa.gov/pbs/pc/facilitiesstandards/

National Capital Planning Commission

http://www.ncpc.gov

"The National Capital - The Urban Design and Security Plan"

http://www.ncpc.gov/publications/UDSP.html

Designing for Security in the Nation's Capital

http://www.ncpc.gov/whats_new/ITFreport.pdf

National Infrastructure Protection Center

http://www.nipc.gov/

National Institute for Occupational Safety and Health: "Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks"

http://www.cdc.gov/niosh/bldvent/2002-139.html

Navy/DOD Force Protection Course

http://atfp.nfesc.navy.mil/training.htm

Pentagon Renovation Program

http://renovation.pentagon.mil

B. Organizations

Building Owners and Managers Association
www.boma.org

Interagency Security Committee
http://www.worldnetdaily.com/resources/govdocs/eos/eo12977.html
http://hydra.gsa.gov/pbs/pc/facilitiesstandards/

International Facility Management Association
http://www.ifma.org/

National Academies of Science and the **Federal Facilities Council** information and publications can be downloaded from
http://www.nationalacademies.org/publications/

The Protection of Federal Office Buildings Against Terrorism
Protecting People and Buildings from Terrorism
Learning from our Buildings

Security Design Coalition   *http://www.designingforsecurity.org/*

Terrorism Research Center   *http://www.terrorism.com/index.shtml*

The Infrastructure Security Partnership
http://www.tisp.org/

C. Recent Studies

GAO "Security Responsibilities for Federally Owned and Leased Facilities"
http://www.gao.gov

GAO "ISC has had Limited Success in Fulfilling its Responsibilities"
http://www.gao.gov
and enter *Report # GAO-02-1004* in search

GAO "Technologies to Secure Federal Buildings"
http://www.gao.gov/new.items/d02687t.pdf

GSA

Smarter Solutions
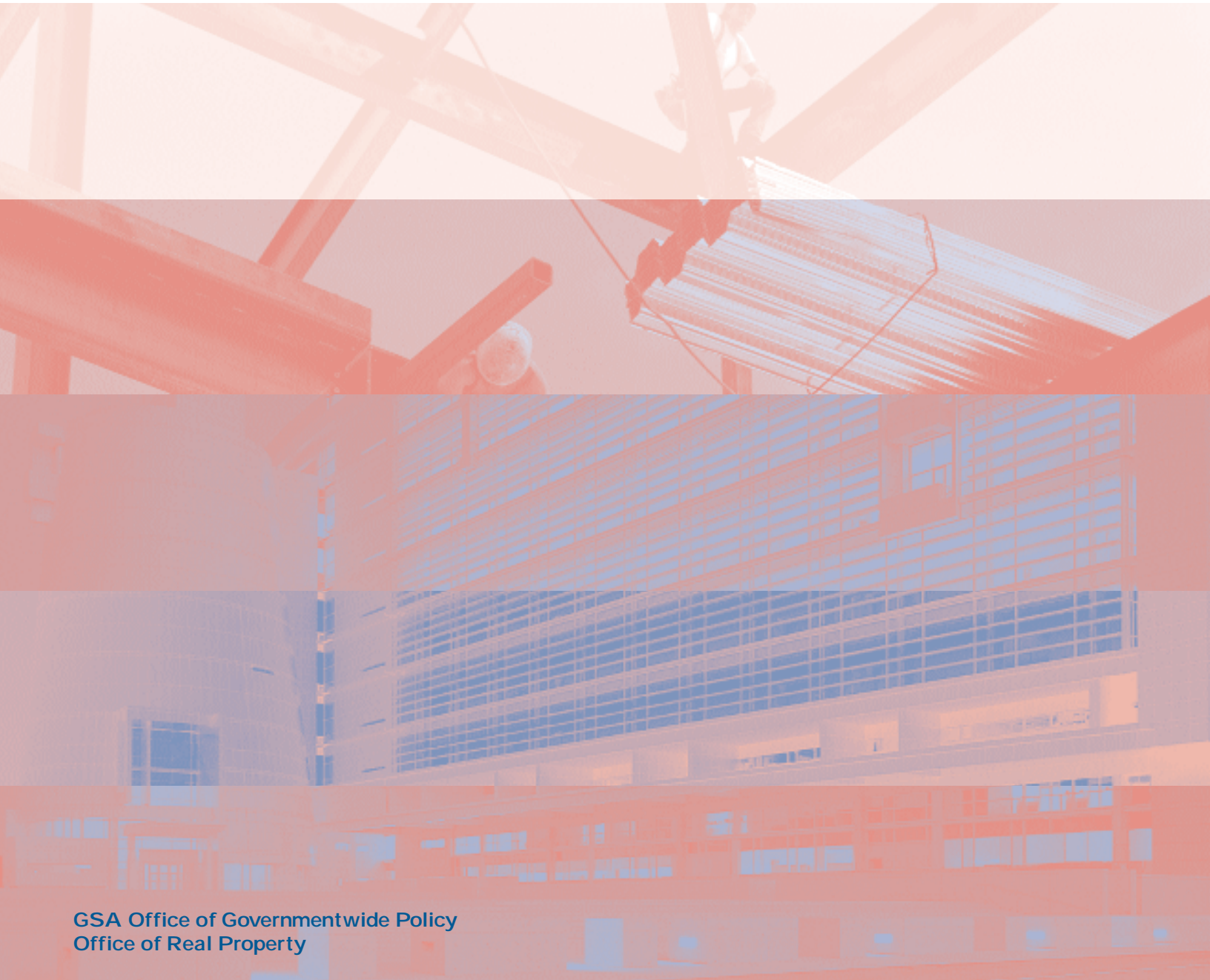
GSA Office of Governmentwide Policy
Office of Real Property