Homeland Security

Office of Intelligence and Analysis/Office of Infrastructure Protection

Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)

(U) Distribution Notice: For any further questions regarding distribution, please contact the Department of Homeland Security, Office of Intelligence and Analysis, Production Management Division at IA.PM@hq.dhs.gov.

(U//FOUO) HITRAC was established in January 2005 to assess risks to domestic critical infrastructure and key resources through enhanced integration of intelligence reporting and analysis with information from respective infrastructure sectors. Analysis of suspicious activity reporting is part of HITRAC's mission to provide strategic, national-level analysis of information reported to the Department.

8 December 2006

Strategic Sector Assessment

(U//FOUO) Government Facilities Sector

*(U) Attention**:** Federal Departments and Agencies, State Homeland Security Advisors, State Emergency Managers, State and Local Fusion Centers, Law Enforcement, Tribal Governments, Information Sharing and Analysis Centers, and the Sector Coordinating Councils.*

*(U) **Warning**: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.*

(U) This product contains U.S. Person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label ^{USPER} and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other USPER information has been minimized. Should you require the minimized USPER information please contact the DHS/I&A Production Management Division at IA.PM@hq.dhs.gov.

(U) Scope

(U//FOUO) This Strategic Sector Assessment is one in a series that provides an overall assessment of the potential terrorist threats to critical infrastructure and key resources, and provides decision makers with the broad, analytically-based threat information necessary to inform investment priorities and program design. It also provides the overarching analytic foundation for incident reports and threat warnings produced by the Department of Homeland Security (DHS) and other Federal partners. This assessment was prepared with input from Federal infrastructure partners and the private sector.

(U//FOUO) This assessment describes DHS' knowledge and provides analysis of current terrorist threats to government facilities sector (GFS) assets within the United States. It also describes known terrorist goals and motives, their potential application to the GFS, vulnerabilities associated with sector facilities and assets, and the potential consequences of an attack.

(U) Key Findings

(U//FOUO) DHS continues to receive information on terrorist threats to the government facilities sector (GFS); however, there is no recent information to suggest terrorist operational planning may be underway in the United States.

(U//FOUO) Al-Qa'ida remains the greatest terrorist threat to the GFS and desires another strike in the United States. An attack against government facilities would fit al-Qa'ida's targeting strategy of causing mass casualties, panic, and economic losses and would further the group's strategic goals.

(U//FOUO) Indigenous Islamic radical groups and lone-wolf individuals driven by al-Qa'ida ideology and anger toward the United States pose a greater threat to U.S. infrastructure—including government facilities—than in the past. Homegrown radicalization is a relatively new phenomenon, which has demonstrated interest in attacking specific sector assets. Various non-Islamic domestic terrorists and radicals also pose a threat to the sector.

(U) Threat Overview

(U//FOUO) Government Facilities Sector: Targeted by Al-Qa'ida

(U//FOUO) In January 2006 Usama Bin Ladin stated that "operations are under preparation and you [Americans] will see them in your homes the minute they are through [*sic*]." DHS assesses that this expressed intent to attack the United States, while not specific, encompasses government facilities. DHS assesses that many sector targets meet al-Qa'ida's targeting criteria, which include causing American casualties and psychological damage to the U.S. population by sowing fear and doubt, making symbolic statements by attacking symbols of U.S. culture and power, and damaging the national economy.

(U//FOUO) **Mass casualties:** DHS analysis of foiled al-Qa'ida plots against U.S. infrastructure demonstrates interest in attacking government facilities assets to inflict mass casualties. According to detainee interviews with al-Qa'ida leader Khalid Shaykh Muhammad, government facilities such as the White House and Capitol building were among the targets considered for the 11 September 2001 attacks. Large number of casualties serves al-Qa'ida by generating media attention, taxing emergency and medical services, and instilling terror in those not directly affected by the attack—as was evident in the 2001 attacks on the Pentagon and World Trade Center.

(U//FOUO) **Attacks against targets of symbolic value:** Terrorists often target GFS assets because they provide unique services, perform sensitive functions, and have symbolic value as physical representations of the national government and the nation as a whole. Khalid Shaykh Muhammad emphasized the importance of selecting targets of symbolic value. Past terrorist attacks against U.S. targets overseas—such as the bombings of the U.S. Embassy and Marine barracks in Beirut in 1983, the simultaneous bombings of U.S. embassies in Kenya and Tanzania in 1998, and the 2000 bombing of the USS Cole in Yemen—reflect this strategy, as do the 11 September 2001 attacks on the Pentagon and the World Trade Center.

(U//FOUO) **Economic damage:** Usama Bin Ladin's statements also demonstrate al-Qa'ida's intent to damage the U.S. economy. In 2003 he lauded the 11 September 2001 hijackers because "they struck at the very heart of the [U.S.] economy." In an October 2004 statement, he quoted the findings of the Royal Institute of International Affairs that the total cost to the United States of the 11 September 2001 attacks was at least $500 billion.

— (U//FOUO) Usama Bin Ladin pointed out that the attacks had cost al-Qa'ida about $500,000 for a million-to-one payoff ratio. He pointed to America's deficit spending for Iraq and Homeland security as "evidence of the success of the bleed-until-bankruptcy plan…[*sic*]."

(U//FOUO) Islamic Extremists and Homegrown Islamic Radicals

(U//FOUO) Antiterrorist operations and strategy have caused al-Qa'ida to decentralize since the 11 September 2001 attacks. The network continues to plot attacks against U.S. and coalition/allied targets, but it now emphasizes influencing other Sunni extremists and homegrown radicals to conduct attacks on their own as well. Indigenous radical groups and lone-wolf individuals driven by al-Qa'ida ideology and anger toward the United States now pose a greater threat to U.S. infrastructure—including government facilities—than in the past.

(U//FOUO) DHS has no information to suggest other Sunni or Shia extremist groups such as HAMAS and Hizballah are currently targeting the sector. These groups however, may find government facilities attractive targets.

(U//FOUO) U.S. infrastructure faces a growing threat from homegrown radicals whose extremist views are informed and inspired by, but not necessarily linked to, al-Qa'ida. These extremists can be U.S. citizens or permanent residents and generally are able to operate freely in U.S. society. Their familiarity with U.S. cultural and social norms makes it more difficult for law enforcement to detect terrorist planning or operations.

(U//FOUO) Non-Islamic Domestic Terrorists and Radicals

(U//FOUO) Various white supremacists, political extremists, and single-issue groups also pose a potential threat to the sector. White supremacist groups use sensitive social and political issues such as immigration to foster radicalization. Political extremists vary across the ideological spectrum from right-wing militia groups to ultra-leftist groups practicing anarchist tactics. Single-issue groups also span the ideological spectrum—to include anti-abortion, animal rights, and ecoterrorists groups—and have the capacity to radicalize and carry out operational activity.

Many such groups have deep antipathy toward government or authority, which can manifest itself in violent acts against its symbols such as government buildings. The 1995 bombing of the Murrah Federal Building in Oklahoma City that killed 168 people is the deadliest incident of domestic terrorism to date.

(U) Sector Overview

(U//FOUO) Because government facilities frequently are collocated with or integrated into facilities in other critical infrastructure and key resources (CI/KR) sectors, the responsibility for protection is based on the facility's predominant use. Exceptions exist based on agreements between the GFS-specific agencies and other sectors. Security for the following facilities is the primary responsibility of the GFS because of these agreements:

(U//FOUO) Personnel-Centric Government Facilities:

- (U//FOUO) Offices and office building complexes.
- (U//FOUO) Government housing.
- (U//FOUO) Correctional facilities.
- (U//FOUO) Embassies, consulates, and border facilities.
- (U//FOUO) Educational facilities.

(U//FOUO) Service-Oriented Government Facilities:

- (U//FOUO) Maintenance and repair shops.
- (U//FOUO) Police, fire, and emergency services stations.
- (U//FOUO) Operations, command, dispatch, and control centers.
- (U//FOUO) Libraries.
- (U//FOUO) Service-oriented land (land associated with service-oriented buildings and structures, including land used for parking areas attached to highways without fuel or maintenance facilities).

(U//FOUO) Research and Development Government Facilities:

- (U//FOUO) Analysis and assessment.
- (U//FOUO) Environmental.
- (U//FOUO) Basic science.
- (U//FOUO) Aerospace.
- (U//FOUO) Weapons.
- (U//FOUO) Research and development related land.

(U//FOUO) Storage and Preservation Government Facilities:

- (U//FOUO) Archive and record centers.
- (U//FOUO) Warehouses.
- (U//FOUO) Weapons and ammunition storage.
- (U//FOUO) Precious metal storage.
- (U//FOUO) Currency storage.
- (U//FOUO) Special nuclear materials and waste storage.
- (U//FOUO) Storage and preservation related land.

(U//FOUO) Military Installations:

- (U//FOUO) Army bases including airfields.
- (U//FOUO) Navy bases including ships and aircraft.
- (U//FOUO) Marine Corps bases including ships and air bases.
- (U//FOUO) Air Force bases including airfields.
- (U//FOUO) Coast Guard bases including ships and air bases.
- (U//FOUO) National Guard facilities including air bases and land-based facilities.
- (U//FOUO) Joint and combined military installations and reservations.

(U//FOUO) Also included are space exploration facilities, government sensor and monitoring systems, and miscellaneous government buildings, structures, and land that do not fit within these classifications.

(U) Vulnerability Overview

(U//FOUO) Government facilities represent attractive and strategically important targets for domestic and international terrorist groups as well as criminals. These assets often are targets because they provide unique services, perform sensitive functions, and have symbolic value. The facilities often are collocated with other CI/KR assets, making them vulnerable to the consequences of an attack on other sector targets. The large size of the sector also makes it difficult to protect. Many facilities rely on contractor security forces for protection and have widely varying standards for security.

(U//FOUO) The sector is vulnerable to both natural and man-made events. Natural events can include meteorological, geological, or biological incidents and typically affect a specific geographic area or are confined. Man-made threats can be intentional—such as criminal acts or malicious behavior, terrorist threats, insider threats, and information warfare—or unintentional—such as equipment or technological failure and human errors.

(U) Scenarios of Concern

(U//FOUO) A historical examination of terrorist attacks worldwide in the last few decades shows the GFS to be the most frequently attacked of the 17 CI/KR sectors. The following is a summary of potential and known threat themes and scenarios of concern that could pose a danger to the government facilities sector:

- (U//FOUO) ***Improvised explosive devices (IEDs)*** and incendiary devices have been used in numerous attacks. Attackers use conventional explosives that can be carried, placed, or delivered. This common attack method can include suicide bombers carrying backpacks, briefcases, packages, or other methods of concealment to hide the explosive. On waterways, divers could deliver the explosive to the target.

- (U//FOUO) ***Vehicle-borne improvised explosive devices (VBIEDs)*** with large amounts of explosives are used extensively in terrorist attacks. The bombing of the Murrah Federal Building in Oklahoma City used a VBIED that was composed of ammonium nitrate and nitromethane. The 1983 bombings of the U.S. Embassy and Marine barracks in Beirut, Lebanon used truck bombs, as did the 1996 bombing of the Khobar Towers in Saudi Arabia. Other VBIED bombings have used smaller vehicles such as cars or light trucks, as was the case in the 1998 bombings of U.S. embassies in Kenya and Tanzania.

- (U//FOUO) ***Maritime attacks*** involve detonating explosives-laden boats near maritime or near-shore targets. Terrorists also could use this method to cause the release of toxic or hazardous material from storage containers or transportation vessels. Well-known examples of this method include the attempted maritime attack on the USS The Sullivans and the bombing of the USS Cole in 2000.

- (U//FOUO) ***Aircraft as a weapon*** was used against government assets in the 11 September 2001 attacks on the Pentagon and World Trade Center (which contained government offices). The potential for use of fixed or rotary wing aircraft as a weapon—particularly against areas that do not have enforced restricted flight zones—remains high. According to Khalid Shaykh Muhammad, other government facilities such as the White House and Capitol buildings were considered targets of the 11 September 2001 attacks.

- (U//FOUO) Several ***biological attack*** scenarios are possible, including the spread of contagious human disease, noncontagious human diseases, or livestock and crop diseases into the population.

  - (U//FOUO) An aerosolized release of a contagious human disease such as smallpox or plague in the lobby of a government office building could propagate through the population by human contact.

- (U//FOUO) Releasing a liquid or dry aerosol of a noncontagious human disease agent such as anthrax through the postal system—similar to the 2001 anthrax mailings to the U.S. Capitol—or through building heating, venting and air conditioning (HVAC) systems would result in potential illness or death among residents of the building.

— (U//FOUO) ***Improvised chemical attack*s** could use readily available chemicals and equipment to generate toxic gases or other chemical hazards, or could involve the use of a stolen chemical weapon. Tactics could include release of gas through aerosol sprayers or release into HVAC systems or other enclosed areas.

— (U//FOUO) ***Nuclear explosives*** would include the detonation of a nuclear weapon acquired from a state-sponsored program or an improvised nuclear device built from weapons-grade nuclear materials. Delivery could be by vehicle, shipping container, or other placement, and would result in mass casualties and—depending on the target—could disrupt the continuity of government.

— (U//FOUO) ***Radiological dispersal device*** attacks combine a radiological source with an explosive or other means of dispersal and could cause casualties or contamination, but on a lesser scale than an actual nuclear explosion.

— (U//FOUO) ***Guided or unguided ranged weapons*** attacks—using man-portable air defense systems, anti-tank weapons, or unguided projectiles—against a building, hardened facility, or perhaps a HAZMAT storage facility are not as likely to produce mass casualties, but could be used to disrupt facility operations.

— (U//FOUO) ***Attack, hostage taking, and assassination is a common terrorist tactic.*** Assaults on assets or confined areas could be used to capture or kill a large number of people or take them hostage. Terrorists conducting an assault against U.S. Consulate Jeddah, Saudi Arabia in 2004 breached the outer perimeter of the compound but failed to make it into the Consulate. The U.S. Ambassador to Sudan was killed in 1973 by the Palestinian group Black September.

(U) Consequence Overview

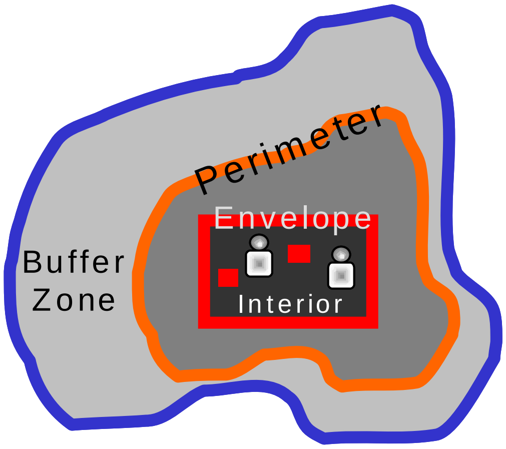
(U//FOUO) A successful attack on the sector would result in significant consequences including undermining national economic security, national public health and safety, and public confidence. Many GFS assets provide unique and critical services, are necessarily open to the public, and can house a large number of people, thereby increasing the effect of any man-made or natural public health and human safety incident. Some GFS assets contain sensitive materials that, if compromised, have the potential to cause mass casualties or public health incidents.

(U) Actions to Reduce Risk

(U) Overall security program planning and administration should ensure that protective programs are comprehensive, coordinated, and cost-effective. This is particularly relevant when different offices may be responsible for the protection of physical assets, cyber systems, networks, and individuals. Over the long term, achieving GFS security goals and objectives should involve building protective considerations into operations through awareness and education. Similar to the behavior-based safety approach used to encourage safe practices by employees, a behavior-based security approach can be used to support prevention of security incidents and protection of government facilities and their contents.

(U) Protection should be applied in layers for optimal effect (see Figure). Layers consider the physical asset and its occupants, contents, cyber systems, and networks:

- (U) **Buffer zone:** The area outside the perimeter of an asset that is typically public property or an area with uncontrolled access.
- (U) **Perimeter:** The border around the asset, system, or network that serves to control access; may be a physical perimeter such as fencing at the property line of a facility or a virtual perimeter such as a firewall.
- (U) **Building envelope:** The structure or barrier that controls access between the perimeter and the interior, including controlled entry points for people, materials, utilities, and information.



(U) Figure: Layers of Protection.

- (U) **Interior:** The area within the envelope that contains assets, systems, networks, and building occupants. Discrete areas in the interior may require additional protective measures.

(U) Protection consists of actions taken to mitigate the overall damage to assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. Consistent with this definition, GFS protective programs should:

- (U) **Deter the threat:** Make assets, systems, networks, and individuals less attractive targets.
- (U) **Mitigate vulnerabilities:** Reduce the target's susceptibility to destruction, incapacitation, or exploitation.

- (U) **Minimize consequences:** Reduce the possible loss resulting from an attack, natural disaster, or accident.

(U) Protective programs cover not only baseline security measures, but also enhancements made in response to elevated threat, overall risk, or an incident and the actions taken during recovery and restoration. As such, protection of government facilities involves a comprehensive approach across the four components of the preparedness spectrum:

- (U) **Prevention:** Actions taken to devalue a facility, detect or deter threats or incidents, and to defend lives and property.

- (U) **Protection:** Actions to minimize consequences and mitigate vulnerability to an attack or other disaster.

- (U) **Response:** Activities designed to enable rapid reaction and emergency response to an incident, such as conducting exercises and having adequate crisis response plans, training, and equipment.

- (U) **Recovery:** Actions that enable government organizations to resume operations quickly and efficiently, such as using comprehensive continuity of government and operations plans developed through prior planning.

(U) **Buffer zones:** Areas surrounding or adjacent to the perimeter of a facility can offer ample room for potential aggressors to observe the physical layout and gather information about structures, traffic patterns, and periods of recurring activity and increased vulnerability. Because many such areas are not under the direct control of the government facility owners and operators, close coordination with local law enforcement agencies is necessary to mitigate risks to the facilities. Buffer zone protection plans (BZPP) can be established to identify and support implementation of protective measures that make it more difficult for aggressors to conduct surveillance, pre-operational activities, and attacks from the immediate vicinity of potential targets. A BZPP should accomplish the following:

- (U) Define the boundaries of the buffer zone outside the perimeter of a potential target.

- (U) Identify specific threats associated with the area surrounding the potential target.

- (U) Analyze the level of risk associated with the potential target.

(U) A BZPP also should recommend measures to reduce the risk in the buffer zone, which may include:

- (U) Visible and frequent police or security patrols.

- (U) Signage delineating the perimeter of the facility, that access is restricted, and that protective surveillance is in place.

- (U) Adequate lighting that makes it more difficult for aggressors to conduct surveillance activities undetected.

- (U) Surveillance to detect hazardous devices or weapons or to prevent suspects' movement toward the weapons or target.

- (U) Physical barriers.

- (U) Coordination with local emergency services in the event of a natural disaster.

(U) **Perimeter protection:** Perimeter protection programs are designed to monitor the immediate surroundings of critical sector infrastructure by using measures to control access into the envelope. Protective programs to mitigate risk at the perimeter include:

- (U) Signage directing vehicles to parking areas, individuals to employee and visitor entrances, deliveries to the shipping and receiving areas, and advising of monitoring and surveillance activities.

- (U) Adequate lighting with emergency back-up that makes it easier to identify suspicious activity or hazardous situations.

- (U) Parking security systems to monitor and regulate vehicles carrying potentially suspicious individuals and packages while deterring threat to connected facilities.

- (U) Duress alarms or assistance stations, including call buttons at key public contact areas and as needed in garages and other areas.

- (U) Monitoring and surveillance such as intrusion detection systems.

- (U) Physical barriers that make threat to protected facilities more difficult.

- (U) Landscaping that provides little cover for potential aggressors.

- (U) Access control, including vehicle inspection checkpoints and individual identification.

- (U) System perimeter security including firewalls for traffic control, address translation and virtual private network (VPN) termination, strong passwords for access control, VPN encryption to create secure connections between the network and remote devices, antivirus scanning devices, and hardware to protect the servers that are exposed to the Internet.

(U) **Envelope protection:** Protective programs to mitigate risk at the envelope, where individuals, materials, utilities, and information enter include:

- (U) Employee and visitor identification, including access control for individuals at designated entrances and exits, security guards, intrusion detection systems, and individual screening.
- (U) Shipping and receiving protocols for screening materials and deliveries received at designated receiving areas.
- (U) Utility conduits containing systems to detect biological, chemical, radiological, or explosive agents.
- (U) Network security layer such as internal local area networks (LANs) and wide area networks, including intrusion detection systems and intrusion protection systems to analyze network traffic more deeply than the firewall; software and hardware, including system monitoring devices that can be set to monitor automatically and continually; and endpoint security that ensures security standards are met by endpoint devices before they are permitted on the network.

(U) **Interior protection:** The interior layer of government facilities infrastructure is distinct from other sector infrastructure layers because it houses the computer systems central to the sector's cyber operations. Databases and LANs within the interior hold sensitive information and regulate firewalls, surveillance systems, and communication lines to protect the facility, its people, and its networks. Protective programs applied within the interior of GFS facilities include:

- (U) Employee and visitor identification and escort systems that prevent unauthorized individuals and personnel from gaining access to sector facilities and networks.
- (U) Surveillance systems such as closed-circuit television and webcam capabilities that monitor activity within a facility and enable security personnel to communicate and respond to disruptions and emergencies.
- (U) Duress alarms or assistance stations, including call buttons in the offices of managers and directors and other areas.
- (U) Signage that instructs individuals how to report suspicious activity or hazardous situations and provides contact information.

- (U) Security for utility closets, mechanical rooms, and telephone closets, including a key system and some type of intrusion detection device.

- (U) Control centers and building management systems for security, operations, and fire prevention and emergencies should be linked by secure information systems. A backup control workstation should be provided in a different location.

- (U) Host security intrusion detection systems used to monitor traffic on individual devices on the network, including routers, switches, desktops, and servers with configurable parameters; host-based monitoring systems; network access control hardware or software to continually monitor each host for infections and harmful applications; device-specific antivirus applications; and stringent group and individual access control through strong passwords and authentication.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the National Operations Center (NOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm, and the NOC can be reached by telephone at 202-282-8101 or by e-mail at HSOC.Common@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document please contact DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) Tracked by:

(U) HSEC-010200-01-05
(U) HSEC-021600-01-05
(U) HSEC-040000-01-05
(U) TERR-010200-01-05
(U) TERR-051600-01-05
(U) TERR-060000-01-05
(U) INFR-160000-01-05