(U) Potential Terrorist Attack Methods

Joint Special Assessment

23 April 2008

Homeland Security
Office of Intelligence and Analysis

Federal Bureau of Investigation

Office of Intelligence and Analysis
Homeland Security

Federal Bureau of Investigation

Joint Special Assessment

(U) Potential Terrorist Attack Methods

23 April 2008

(U) Prepared by the DHS/Homeland Infrastructure Threat and Risk Analysis Center and the FBI/Threat Analysis Unit. Coordinated with the DHS/Transportation Security Administration, DHS/United States Coast Guard, DHS/National Cyber Security Division/United States Computer Emergency Readiness Team, United States Department of Agriculture/Food and Drug Administration, Defense Intelligence Agency, and Environmental Protection Agency. The Interagency Threat Assessment and Coordination Group (ITACG) reviewed this product from the perspective of our non-federal partners.

(U) Table of Contents

(U) Scope

(U//FOUO) Under the National Infrastructure Protection Plan, the Department of Homeland Security's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) has the responsibility to produce assessments that support the strategic planning needed to enhance the protection and preparedness of the Nation's critical infrastructure and key resources (CIKRs). HITRAC analyzed information about terrorist attack capabilities, goals, and objectives to assess the potential terrorist attack methods that might be used against CIKRs.

(U//FOUO) This paper is complementary to the 2007 *Strategic Homeland Infrastructure Risk Assessment (SHIRA*). The SHIRA analysis is based on a defined set of 15 attack methods that were identified based on known terrorist capabilities, analysis of terrorist tactics, techniques, and procedures, and intelligence reporting on assessed, implied, or stated intent to conduct an attack. This assessment discusses the attack methods in alphabetical order and implies nothing about the probability of one attack method being chosen over another.

(U) Identified Terrorist Attack Methods

(U) Aircraft as a Weapon
(U) Biological Attack: Contagious Human Disease
(U) Biological Attack: Noncontagious Human Disease
(U) Biological Attack: Livestock and Crop Disease
(U) Chemical Attack
(U) Cyber Attack
(U) Food or Water Contamination
(U) Hostage-Taking
(U) Improvised Explosive Device
(U) Maritime Vessel as a Weapon
(U) Nuclear Attack
(U) Radiological Dispersal Device
(U) Standoff Weapons: Guided
(U) Standoff Weapons: Unguided
(U) Vehicle-Borne Improvised Explosive Device

(U//FOUO) This attack method compendium provides a broad overview of methods terrorists might use in attacks against Homeland critical infrastructure. Innovation is a hallmark of terrorism, and an actual attack may not mirror past attacks. The compendium offers a basic description of each of the 15 attack methods, including definition, background, key components, and possible methods of employment. The compendium is not intended to provide an all-encompassing or in-depth look at terrorist intent and capability to conduct attacks against specific CIKRs, but rather to provide general overviews to further inform DHS critical infrastructure protection partners of the potential threats they could face.

(U//FOUO) DHS understands that each infrastructure asset is unique and has different vulnerabilities to various types of terrorist threats. It is likely that only a subset of the 15 attack methods presented will be pertinent to any particular site. Alternatively, additional attack methods or threats not addressed in this paper may be of higher concern to an individual infrastructure asset.

(U) Aircraft as a Weapon

(U//FOUO) Past attacks and disrupted plots demonstrate terrorists' interests in using aviation as an attack method. To lower the overall risk from this attack method, the Federal Government has placed high emphasis on preventing aircraft from being commandeered. Aircraft as a weapon presents unique challenges for security at the facility level. Vulnerability to this attack method is high across most infrastructure sectors, since it is extremely difficult to provide adequate countermeasures at the critical infrastructure/key resources (CIKRs) sites. Successful attacks could cause severe consequences.

(U) Definition

(U//FOUO) The attack method, aircraft as a weapon, is the terrorists' use or control of an aircraft as a means to attack infrastructure targets directly. The aircraft could be cargo aircraft, gliders, helicopters, large or small commercial passenger aircraft, privately owned aircraft of any size, or unconventional airborne vehicles, such as lighter-than-air vehicles.

(U) Background

(U//FOUO) The 11 September 2001 attacks demonstrated the destructiveness, lethality, and potential catastrophic consequences of terrorists' use of aircraft as a weapon. Enhanced security measures and heightened passenger sensitivity regarding aviation security make it more difficult for terrorists to conduct an 11 September 2001-style attack, but terrorists likely will continue to seek innovative ways to conduct large-scale attacks using aircraft.

(U) Key Components

(U//FOUO) For terrorists to conduct an attack on infrastructure using an aircraft, they must be able to accomplish the following: evade or overcome internal and external security measures, gain control of the aircraft on the ground or in flight, fly or dictate the flight of the aircraft, and maintain control of the aircraft to the intended target.

— (U//FOUO) Terrorists may attempt to bypass rigorous security at commercial passenger airports with innovative weapons or operatives. As demonstrated by the 2006 London plot to detonate liquid explosives on board airlines, terrorists will continue to seek creative ways to pass through security and to reduce the potential for detection.

— (U//FOUO) Commercial passenger aircraft have been used in the past; however, terrorists may attempt to gain access to and control over nonpassenger

commercial or privately owned aircraft for which overall security may not be as robust.

— (U//FOUO) Terrorists conceivably could attempt to coerce a pilot or seek assistance from an employed pilot with terrorist connections, but more likely they will choose to fly the aircraft themselves, as demonstrated in the 11 September 2001 attacks, in which each team of hijackers included a trained pilot. Basic navigation training is especially important for the hijackers to find their intended target. In addition, since this attack method is almost certainly a suicide mission, terrorist groups must have capable and trained operatives who are cognizant of the mission's objective and are willing to die for their cause.

— (U//FOUO) The terrorists must be able to maintain control of the aircraft until it hits its target. As demonstrated by the events aboard United Airlines Flight 93 during the 11 September 2001 attacks, terrorists must have some way to control passengers to commandeer a commercial passenger aircraft. U.S. Government security measures since 11 September 2001, such as better screening of luggage and passengers and enhancing cockpit security, as well as the increased proactive attitudes of passengers, make this attack method much more challenging for terrorists.

(U) Methods of Employment

(U//FOUO) **Commandeering a commercial aircraft:** Terrorists may use a cargo, commercial, fixed-wing, or passenger aircraft. Terrorists most likely would obtain an aircraft by hijacking using concealed weapons, but it also is possible that a commercially or privately employed pilot with terrorist connections could use this tactic. In addition, to avoid U.S. airline security, terrorists may hijack a foreign aircraft not originating from or destined for a U.S. airport and divert it to attack a U.S. target.

— (U//FOUO) In September 2001, al-Qa'ida terrorists hijacked four U.S. commercial airliners and succeeded in using three of them as weapons against the Pentagon and the two World Trade Center towers. The fourth aircraft was crashed into a field in Pennsylvania when the passengers attempted to take control of the plane. Nearly 3,000 people were killed in the attacks.

— (U//FOUO) In 1994, an employee at a shipping company boarded a California-bound cargo flight in Memphis armed with two hammers, a knife, two mallets, and a spear gun—all concealed within a guitar case. He attempted to hijack the aircraft and crash it into the shipping company's headquarters. The flight crew succeeded in restraining him and returned the plane safely to the ground.

— (U//FOUO) In 1994, four members of the Armed Islamic Group armed with automatic weapons, explosives, and hand grenades boarded an Air France Flight

departing Algeria to Paris, possibly intending to fly the plane into the Eiffel Tower. All four hijackers were killed when French security forces stormed the aircraft.

— (U//FOUO) In 1974, an unemployed tire salesman attempted to hijack a plane from Baltimore–Washington International Airport to crash it into the White House. The attacker shot and killed one police officer and injured both pilots. The attacker was injured in a standoff with police and committed suicide before officers could gain entry to the plane.

(U//FOUO) **Use of private aircraft:** Terrorists could use a purchased, rented, or stolen private aircraft. Chartered or leased aircraft range from a small, single-engine plane to an aircraft the size of a Boeing 747. The airplane likely would be smaller than most commercial aircraft, but it is possible for terrorists to load the plane with additional explosives, increasing its destructive potential.

— (U//FOUO) In 2002, a 15-year-old student pilot acting on his own crashed a stolen small aircraft into a financial building in downtown Tampa, Florida. The pilot left a note expressing solidarity and sympathy for the cause of al-Qa'ida and its attacks on the Pentagon and the World Trade Center towers. The pilot was the only fatality.

— (U//FOUO) In 1994, a 38-year-old man crashed a stolen small aircraft onto the White House lawn. The pilot, who was not connected to any extremist organizations, was intoxicated and faced an array of financial, legal, and marital problems. The pilot, the sole casualty, was killed on impact.

(U//FOUO) **Use of unconventional airborne vehicles:** Aircraft such as gliders, gyrocopters, hot air balloons, powered parachutes, or remote-controlled aircraft would be relatively easy to obtain and use, but their kinetic strike capabilities are limited. Incorporation of destructive compounds or explosives would be needed to inflict substantial damage on people and property.

(U) Biological Attack

(U//FOUO) A biological attack—unlike a chemical, conventional, or nuclear attack—may go undetected for hours, days, or weeks (depending on the agent) until victims begin to show symptoms of disease. If an attack is not apparent immediately, local health care workers probably would be the first to detect it by observing unusual patterns of illness. Early warning systems monitoring for airborne pathogens may provide early indications of an attack. Detection of a biological attack is likely to be accompanied by uncertainties among law enforcement and medical personnel about crucial facts, such as the exact location or extent of the initial release, the type of biological agent used, the number and

location of people exposed, and the likelihood of additional releases. Identifying the point of release of a biological attack is much more difficult than identifying the source of a conventional terrorist attack.

(U//FOUO) A biological weapon is a device designed to cause disease intentionally through dissemination of bacteria, biological toxins, or viruses. Biological agents can be spread through the air, by direct contact, and in food and water. Militaries typically have controlled biological weapons, although criminals and terrorists have a long history of using biological agents. This paper discusses three biological attacks: contagious human disease, noncontagious human disease, and livestock and crop disease.

(U) Contagious Human Disease

(U) Definition

(U//FOUO) A biological weapon is considered contagious when a disease-producing microorganism (pathogen) is transmitted from an infected person to others by direct or indirect contact. Two major categories of pathogens are bacteria and viruses:

— (U//FOUO) **Bacteria** are single-celled microorganisms that live in the bodies of plants and animals, organic matter, soil, or water. Pathogenic bacteria damage surrounding host tissues with toxins. *Yersinia pestis,* the causative agent of plague, is a contagious bacterium in its pneumonic form. When a person has pneumonic plague, droplets containing the plague bacteria can be spread into the air. This is a less common but much more dangerous form of the disease than bubonic plague. Other examples include multidrug-resistant tuberculosis and extensively drug-resistant tuberculosis. Rickettsia is a type of bacteria that causes diseases such as typhus.

— (U//FOUO) **Viruses** are submicroscopic infective agents capable of growth and multiplication only in living cells. Viruses damage living tissues by destroying individual cells in the act of replication. Variola virus, the causative agent of smallpox, and filoviruses, such as Marburg and Ebola, are examples of viruses that could theoretically be used in bioterrorism attacks.

(U//FOUO) Biological agents can be extremely diverse in their mode of symptoms, transmission, and treatment. For example, symptoms from an influenza virus infection can take 48 hours to appear, whereas symptoms from a smallpox virus infection can take as long as 17 days. In addition, some agents are easily transmissible through the air, such as the influenza virus; but others, such as hemorrhagic fever viruses, are not.

(U) Background

(U//FOUO) Contagious biological agents have been used in attacks throughout history. Terrorist groups have shown interest in using biological agents to cause chaos and mass

casualties. Past natural pandemics of contagious diseases, such as the Black Plague, have caused mass casualties along with economic and social disruption, which are key terrorist goals.

(U//FOUO) According to the Centers for Disease Control and Prevention, seven biological agents are considered Category A, the highest priority agents that could cause a threat to national security. Of these seven agents, three fall into the contagious biological agent category: *Yersinia pestis* ("plague"), *Variola major* ("smallpox"), and some hemorrhagic fever viruses, such as Ebola.

(U//FOUO) Several countries conduct research on biological agents. Many agreements and treaties are in place around the world to limit proliferation of such material, but it is possible that terrorist groups could exploit biological research laboratories to obtain agents for offensive purposes.

(U) Key Components

(U//FOUO) Key components in the ability to conduct attacks using contagious agents include the following:

— (U//FOUO) The possession of a viable pathogenic bacteria or virus in sufficient quantity to cause a communicable disease. Biological agents can be stolen from laboratories or repositories or isolated from sources in nature.

— (U//FOUO) The ability to culture or grow agents in quantity. Some agents would require further processing to use in an attack. Growing a virus would be more challenging and require a higher degree of technical knowledge than growing bacteria.

— (U//FOUO) An effective delivery mechanism or means of dissemination.

(U) Methods of Employment

(U//FOUO) A contagious human disease is unlikely to be used against specific infrastructure facilities (unless terrorists are targeting the public health sector), but more likely targeted at population centers. Given an attack, however, a contagious human disease could spread across geographic areas, and CIKRs sectors likely would be affected in some way. Methods of employment include the following:

(U//FOUO) **Agent release in an enclosed space:** The adversary could use an aerosol generator to disperse a dry or liquid agent in a cloud or vapor. Releasing the agent in an enclosed space allows greater exposure to individuals within, while protecting the agent from humidity, wind currents, and ultraviolet radiation, all of which can decrease its potency.

— (U//FOUO) Effective aerosol generators are available for purchase or could be improvised. A terrorist also could use a facility's constantly circulating heating, ventilation, and air conditioning (HVAC) system as a passive aerosol generator. It is plausible that certain locations in the system where high air volume and speed coincide could aerosolize a biological agent and disperse it throughout a facility.

(U//FOUO) **Introduction of an infected individual or "vector" in a public area:** Use of a human vector requires a terrorist to infect one of his own operatives or an unwitting victim with a contagious disease and then deploy that person to infect others. Prolonged, close contact with individuals—and contact with inanimate objects such as doorknobs, handrails, or light switches—is known to spread some infectious agents, although mass casualties likely would not result from this method. Infected animals or insects also could act as vectors if released into an environment where they could transmit the disease to humans.

— (U//FOUO) The bacterium that causes plague, *Yersinia Pestis,* is primarily a rodent pathogen. The bacteria are spread to humans through direct contact with a wild rodent or an infected flea. Plague persists in many parts of the world today, with several hundred cases being reported to the World Health Organization each year, mostly from Africa. Cases do occur in the United States. Between 1957 and 1999, 45 confirmed plague cases originated in Colorado, nine of which resulted in death.

(U//FOUO) The susceptibility and immune response of hosts can vary because of individual characteristics, adding a variable to the period of contagiousness and the transmission pattern through the population.

(U//FOUO) **Introduction of an "endemic agent" using methods that would conceal malevolent origin:** This method requires the adversary to introduce a pathogen in a way that closely resembles a natural outbreak of the disease. Epidemiologists understand the normal rates at which natural disease outbreaks spread, and if an outbreak grows at an accelerated rate, it could indicate an intentional pathogen release. Attackers intending to covertly disseminate an endemic agent probably will use vectors native to the targeted area.

(U) Noncontagious Human Disease

(U) Definition

(U//FOUO) A biological weapon is considered noncontagious—although still capable of causing disease—if the pathogens are not transmissible through direct or indirect personal contact. Major pathogens are bacteria, toxins, and viruses:

— (U//FOUO) **Bacteria** are single-celled microorganisms that live in the bodies of plants and animals, organic matter, soil, or water. Pathogenic bacteria damage

surrounding host tissues with toxins. *Bacillus anthracis,* the causative agent of anthrax, is an example of this type of bacteria, as is *Francisella tularensis,* a bacterium found in animals (especially rabbits and rodents) that causes tularemia. Bubonic plague, caused by the bacterium *Yersinia pestis,* occurs when an infected flea or rat bites a person or when materials contaminated with the bacterium enter through a break in a person's skin.

— (U//FOUO) **Toxins** are poisonous substances produced by living cells or organisms. The bacterium *Clostridium botulinum* produces a toxin that causes the muscle-paralyzing disease botulism.

— (U//FOUO) **Viruses** are submicroscopic infective agents capable of growth and multiplication only in living cells. Viruses damage living tissues by destroying individual cells in the act of replication. Venezuelan equine encephalitis, a mosquito-borne disease that infects equines and humans, is caused by a virus.

(U//FOUO) Biological agents can be extremely diverse in their mode of transmission, symptoms, and fatality rates. For example, Q fever, a disease caused by the bacteria *Coxiella burnetii,* which is transmissible from animals to humans, may kill 2 percent of untreated cases, whereas an untreated pulmonary anthrax infection kills almost 100 percent of its victims.

(U//FOUO) As living organisms, many biological agents can be killed or inactivated when exposed to ultraviolet radiation or high temperatures. *Bacillus anthracis*—the causative agent for anthrax—is of special interest as a biological agent because the bacteria's dormant spore form is extremely resistant to adverse environmental conditions for decades.

(U) Background

(U//FOUO) Noncontagious pathogens have caused sickness and death in the United States and around the world. Incidents involving noncontagious pathogens have social impacts such as inducing fear in the population and causing economic damage. As previously mentioned, the Centers for Disease Control and Prevention categorizes seven biological agents as Category A, the highest priority agents that could cause a threat to national security. Four are the noncontagious biological agents: anthrax, botulinum toxins, plague (bubonic plague), and tularemia. Bubonic plague is not directly transmissible, although it can spread throughout the body and cause the pneumonic form of plague, which is transmissible.

(U//FOUO) Several countries conduct research on biological agents. Many agreements and treaties are in place around the world to limit proliferation of such material, but it is possible that terrorist groups could exploit this capability to obtain agents for offensive purposes.

(U) Key Components

(U//FOUO) Key components in the ability to conduct attacks using noncontagious agents include the following:

— (U//FOUO) Possession of a viable noncommunicable bacterium or virus that can cause disease. Biological agents can be stolen from laboratories or repositories or isolated from sources in nature.

— (U//FOUO) The ability to culture or grow agents in quantity. Some agents would require further processing to use in an attack. Growing a virus would be more challenging and require a higher degree of technical knowledge than growing bacteria.

— (U//FOUO) An effective delivery mechanism or means of dissemination.

(U) Methods of Employment

(U//FOUO) **Rudimentary nonairborne dispersal:** Terrorists could manually disperse biological agents in solid or liquid form.

— (U) In 2001, letters containing anthrax were mailed to the New York City offices of one major television network and a newspaper, and to another media office in Florida. Two weeks later, two anthrax-filled letters were mailed to the offices of two U.S. Senators. In addition, postal facilities in the Washington, D.C. area and other locations were affected by the mailings. The FBI continues to investigate these attacks, which caused five deaths.

(U//FOUO) **Rudimentary airborne dispersal:** Terrorists could use rudimentary means to deliver dry or liquid biological agents through the air.

— (U) In April 1979, a Soviet biological weapons facility in the city of Sverdlovsk, Ukraine (now Yekaterinburg) accidentally released anthrax spores into the surrounding area, killing 94 people. A technician forgot to place a new filter in a dryer, after the old filter was removed. This procedural lapse resulted in an aerosol release of agent into the atmosphere when the dryer was restarted.

— (U) In 1939 and 1940, Japanese Army Biological Warfare Unit 731 in Manchuria dropped plague-infested fleas and plague-saturated rice by airplane onto the Chinese population of Chekiang Province. The resulting human epidemics of noncontagious bubonic plague killed thousands of Chinese civilians.

(U//FOUO) **Aerosolized release in an open area:** Terrorists who have the technical capability could attempt to release an agent into a large populated area using an aerosol device. A modest level of technical know-how is needed to optimize aerosol dissemination, but even relatively crude devices could have an impact.

— (U) In July 1993, the Japanese cult, Aum Shinrikyo, attempted to spread anthrax in Tokyo using a sprayer system on the roof of a building. The anthrax was disseminated over four days. The accidental use of a vaccine strain of anthrax was the primary reason the attack caused no human casualties.

(U//FOUO) **Aerosolized release in an enclosed space or public building:** Terrorists who have the technical capability could attempt to release an agent into an enclosed space. They could use an aerosol generator, or a more rudimentary device that relies on a facility's HVAC system to spread the agent. Releasing an agent in an enclosed space would reduce its vulnerability to ultraviolet radiation and help ensure the aerosol is sufficiently concentrated to cause casualties.

(U//FOUO) **Injection:** Terrorists could inject an agent directly into the bloodstream of an individual. In 1978, Bulgarian dissident Georgi Markov was assassinated with a ricin toxin injected using the tip of an umbrella.

(U) Livestock and Crop Disease

(U) Definition

(U//FOUO) Disease-producing microorganisms, also called pathogens, can infect livestock and crops. Types of diseases that may have plausible uses in biological attacks on livestock and crops include the following:

— (U//FOUO) **Animal diseases:** Foot and mouth disease (FMD), hog cholera, rinderpest, and swine fever.

— (U//FOUO) **Plant diseases:** Fungi, to include anthracnose, blight, damping-off, leaf spot, root and crown rots, smut, vascular wilts, and rust, to include soybean and wheat rust.

— (U//FOUO) **Zoonotic diseases:** Anthrax, avian influenza, brucellosis, hantavirus, and plague have the potential to harm animals and humans.

(U) Background

(U//FOUO) An attack on crops or livestock could create complex challenges for the Federal Government, first responders, and industry. Potential biological agents needed to carry out an attack are held in laboratories and repositories and may even be present in the environment, making these locations potential sources from which terrorists might acquire these pathogens. In addition, the agricultural infrastructure of the United States may be more vulnerable to the deliberate use of biological agents owing to factors such as the globalized food and agriculture systems, processes, and products and terrorists' attempts to develop or acquire biological agents.

(U//FOUO) A major agroterrorism incident would have significant consequences for the United States. With the exception of those causing zoonoses, livestock and crop pathogens are harmless to humans. It is often difficult to distinguish a terrorist attack from a natural outbreak, and economic damage from an attack could be severe. The loss of profits and costs associated with cleanup could be high, and subsequent import restrictions or foreign trade sanctions could gravely affect U.S. industry and trade. A loss of public confidence in the safety of the food supply also could lead to significant economic consequences and have behavioral and psychological impacts.

— (U//FOUO) Documents recovered in April 2002 in Afghanistan indicated that prior to 11 September 2001, al-Qa'ida had an interest in agroterrorism agents. One document contained a list of high-consequence animal disease agents, such as the highly pathogenic avian influenza, FMD virus, and hog cholera virus.

— (U) According to U.S. Department of Agriculture officials, a single case of FMD in the United States could cause U.S. trading partners to prohibit imports of live animals and animal products, resulting in losses of between $6 billion and $10 billion a year until the United States eradicated the disease and regained disease-free status.

— (U) Since the mid-1990s, the natural spread of *Phytophthora ramorum,* causal agent of sudden oak death, has caused the destruction of millions of dollars' worth of nursery stock and led to significant costs associated with eradication efforts in forests in California and Oregon and in infested nurseries in more than 40 states. These costs were borne by the growers and by U.S. taxpayers through federal and state agencies.

(U) Key Components

(U//FOUO) To execute an attack on crops or livestock, terrorists must have the ability to obtain a pathogen and a means to disperse it to the intended target.

(U//FOUO) Terrorists could acquire a pathogen by isolating it from the environment where it naturally occurs, obtaining it from a state sponsor, or ordering or stealing it from a laboratory culture collection. The culturing of many animal and plant diseases from the environment is less risky than isolating human pathogens because with animal diseases, terrorists run little-to-no risk of contracting the disease. A terrorist could obtain an infected animal or plant, and after modest processing, have a sample of the pathogen. Many plant pathogens could be obtained from the environment in areas where they are endemic, with little expertise needed.

— (U) In late August 1997, farmers in New Zealand attempted to eradicate rabbits infesting their crops by illegally introducing rabbit hemorrhagic disease into the environment and, without any special equipment, were able to cultivate the virus and then disseminate it by contaminating vegetables left out for the rabbits.

(U//FOUO) Terrorists could disperse a pathogen to targets in a variety of ways to include an aerosol dispersed by a spray mechanism or air currents, human application, or an infected animal. For example, American cattle feedlots handle large numbers of livestock at once; therefore, aerosol dispersal may not be necessary to contaminate livestock because of a high degree of contact between animals and the high transmissibility of certain agents.

(U) Methods of Employment

(U//FOUO) **Introduction of an animal pathogen at an exchange node:** Livestock are brought to central locations for a variety of reasons, such as auctions and county fairs. This practice potentially provides terrorists with an opportunity to infect many livestock that subsequently would be transported elsewhere, where they could infect other animals. In addition, certain types of livestock, such as pigs, often are bred, and slaughtered in different locations. A pathogen, whether introduced through human application or a contaminated vector, could spread quickly through a region through such exchanges.

(U//FOUO) **Introduction of an animal pathogen at a large farm or ranch:** Livestock often are housed in highly concentrated populations; large poultry producers, for example, house tens of thousands of birds in a single facility. A virulent pathogen such as highly pathogenic avian influenza could infect a large number of poultry fairly quickly. Wildlife could spread the disease further by visiting the infected farm and then visiting other farms along a migration route. Even if the pathogen did not spread beyond the site of introduction, the emergence of a foreign animal disease would affect all producers directly because trading partners may not distinguish between properties; all trade in that commodity could be suspended.

- (U) FMD can cause serious animal welfare issues, and even a single outbreak in livestock can have devastating consequences. In February 2001, an outbreak of FMD was confirmed in the United Kingdom. The disease spread rapidly and lasted for 10 months. During this time, 2,034 outbreaks occurred extending to 10,124 farms. The economic consequences included the slaughter of more than 6 million animals and a loss of revenue from tourism. Outbreaks also occurred in France, Ireland, and the Netherlands during the same year. In August 2007, the United Kingdom faced another FMD outbreak.

(U//FOUO) **Introduction of an agent from an international source:** Terrorists may attempt to introduce an agent into livestock feed during its overseas production, storage, or transportation, where access may be easier and detection less likely. This attack method would require knowledge of which agents would remain effective through transport and to the destination of the product.

- (U//FOUO) In 2000, a nonmalicious, simultaneous outbreak of FMD in Japanese and Korean cattle was thought to have been introduced by hay imported from

China. According to one study, the direct costs of the outbreaks were $15 million in Japan and $433 million in the Republic of Korea.

— (U) *Ralstonia solanacearum* race 3 biovar 2 is a bacterial pathogen not known to occur in the United States. It causes a wilt disease in several important agriculture crops such as eggplant, peppers, potatoes, and tomatoes. The disease it causes is known as bacterial wilt, brown rot of potato, or Southern wilt. The bacterium was inadvertently introduced to several states via greenhouse-produced geraniums imported from Guatemala in 2004 and Kenya in 2003. The disease subsequently was eradicated; however, approximately 450 facilities in 41 states received suspect geraniums from the Guatemalan facility. Global damage estimates on bacterial wilt of potatoes currently exceeds $950 million annually.

(U//FOUO) **Introduction of a zoonotic pathogen:** An attack using a zoonotic pathogen, one that is communicable from animals to humans under natural conditions, could have consequences far different from a nonzoonotic attack. Reported cases of zoonoses are monitored closely because of the danger zoonotic pathogens pose to humans, potentially making it more difficult for terrorists to employ this method of attack without early detection. Incubation time of the pathogen is another factor to consider; a long incubation time would make early detection more difficult.

— (U//FOUO) As of February 2007, highly pathogenic avian influenza (H5N1) had affected 57 countries across the globe and claimed the lives of 167 out of 273 affected persons. More than 95 million birds have been destroyed, and bans have been placed on imports of chicken coming from stricken countries.

— (U//FOUO) In the United States, different avian influenza viruses caused outbreaks among poultry in 2003 and 2004. In February 2004, an outbreak of highly pathogenic avian influenza (H5N2) was detected in a flock of 7,000 chickens in Texas.

(U//FOUO) **Introduction of a plant pathogen into crop fields:** A pathogen could be disseminated in liquid or solid form. A pathogen in a liquid medium could be dispersed over a crop field by manual application, a spray mechanism (including ultra-low volume aerial applications using crop dusters), or as a result of an explosion, although an explosion risks simultaneously destroying much of the pathogen. Dry agent could be spread over fields on air currents, and the prevailing wind could carry the pathogen kilometers to other locations and eventually create a widespread infestation.

— (U) In late 2004, the soybean rust pathogen, a fungus that is easily spread through wind-borne spores, was introduced for the first time into the southern United States. Pathologists strongly suspect that Hurricane Ivan, which hit the southern coast in September 2004, is responsible for the spread of the disease from South America.

(U//FOUO) Two of the main crop diseases identified as potential biological weapons are rice blast and wheat stem rust. Rice blast, a fungal disease, spreads rapidly; the spores can float through the air infecting other plants. Breeding resistant rice strains is difficult because 219 types of this fungus exist. Wheat stem rust spores also are dispersed easily in the air, but the use of resistant wheat strains limits its effectiveness as a biological weapon.

(U) Chemical Attack

(U//FOUO) The use of toxic chemicals in terrorist attacks could produce severe consequences. The continued interest in chemical attacks is demonstrated by the attempts to acquire chemical agents by militants, and the high-profile terrorist attacks in Iraq using chlorine-based improvised explosive devices.

(U) Definition

(U) A chemical attack is the spreading of chemicals with the intent to do harm. The Chemical Weapons Convention defines a chemical weapon as "any toxic chemical or its precursor that can cause death, injury, temporary incapacitation, or sensory irritation through its chemical action." A variety of chemicals could be used in an attack, to include toxic commercial and industrial chemicals and warfare agents developed for military use. The chemical could be used in various forms or states—such as gas, liquid, or solid. The toxicity of chemicals varies greatly; some are acutely toxic (causing immediate symptoms) in small doses, others are not toxic at all. Chemicals in liquid or vapor form generally create greater exposure than chemicals in solid form.

(U) Background

(U//FOUO) First used in World War I, chemical weapons initially drew from existing industrial chemicals. State programs rapidly expanded until the Chemical Weapons Convention entered into force and was ratified by more than 160 nations in 1997 with the goal of eliminating state development, production, storage, and use of chemical weapons. The use of chemicals as a terrorist weapon was highlighted by the Aum Shinrikyo (now called Aleph) cult's 1995 sarin nerve gas attack on the Tokyo subway. Reporting indicates terrorists have been and may continue to be interested in using chemicals in attacks.

- (U//FOUO) Iraqi insurgents have tried repeatedly since October 2006 to enhance the effects of vehicle-borne improvised explosive devices (VBIEDs) with chlorine. On 28 January 2007, a VBIED attack against a police compound that involved a truck carrying a chlorine tank and explosives killed 16 people, although no deaths were caused by the chlorine gas. Personnel in the area reported a strong odor of chlorine and suffered symptoms consistent with chemical exposure.

— (U) In 1995, Aum Shinrikyo attacked the Tokyo metro with bags of liquid sarin that it had manufactured killing 12 and causing more than 5,000 to seek treatment.

— (U) In 1994, Aum Shinrikyo released a cloud of sarin from a converted refrigerator truck in Matsumoto, Japan in an attempt to assassinate three judges residing in a nearby dormitory. The judges survived the attack, but seven people were killed and hundreds were hospitalized.

(U) Key Components

(U) To carry out a chemical attack effectively, terrorists must obtain the chemical agent—whether through production, purchase, or theft—and disperse the agent to the intended targets.

(U) How terrorists obtain a chemical depends on which chemical is sought. Terrorists could buy or steal some chemicals from legitimate businesses. As demonstrated in Iraq, deployment of an improvised chemical weapon involved only stolen chlorine paired with an explosive. Other deadly and potent chemicals and even some of their precursors are not as readily available, and terrorists would have to develop a capability to produce the chemical themselves. Successful synthesis would depend on the availability of precursors, the maker's access to processing and storage equipment, and technical know-how.

(U) The ability to disperse the chemical also determines the effectiveness of an attack. A terrorist group may be able to access hazardous chemicals; however, without an effective dispersal mechanism, the success of the attack will be limited and the potential consequences diminished.

— (U) Step-by-step manuals for the employment of chemicals as weapons can be found on a number of jihadist websites. One website stated the following:

> *(U//FOUO) Fatal poisons are among the most lethal and terrifying weapons, and the least costly. If it were not for the difficulty in ensuring delivery of sufficient quantities of this lethal substance, and in protecting the safety of its manufacturer, carrier, and user, it would be the most favorite tool [of the mujahidin].*

(U) Methods of Employment

(U//FOUO) Several methods of employment are possible in a chemical attack. The routes of exposure, the meteorological conditions during an attack, and the type of delivery mechanisms all affect the severity of an attack.

(U) **Routes of exposure:** The ways in which people come into contact with a hazardous substance include breathing (inhalation), eating or drinking (ingestion), contact with the

skin (dermal contact), or injection. It is possible to have multiple routes—dermal exposure and inhalation—in the same attack.

(U) **Meteorological conditions:** Meteorological conditions—humidity, temperature, and wind—influence the effectiveness of toxic chemicals in the air or on the ground. Many environmental variables affect the speed of diffusion of a chemical agent. Toxic chemicals released in an enclosed space (airport terminals, office buildings shopping centers, subways) could reach a high concentration, injuring or killing a large number of people. In an open area, a chemical agent vapor will become less concentrated through diffusion and mixing, requiring the release of greater quantities to produce a similar number of casualties.

(U//FOUO) Release of a Chemical Agent into an HVAC System

(U//FOUO) Whether used in conjunction with an aerosol generator or by rudimentary liquid or powder diffusion, the high airflow of an HVAC system could disperse chemicals throughout an enclosed area quickly.

(U//FOUO) One jihadist pamphlet recommends targeting bars serving alcohol, cinemas, dancing clubs, government buildings, hospitals, investment businesses, religious centers, restaurants, schools, shopping malls, and theaters. The pamphlet also specifically mentions targeting enclosed areas and HVAC systems.

(U//FOUO) **Delivery mechanisms:** Terrorists could conduct a chemical attack by release in an HVAC system, or by aerosolized, explosive, or powder dispersal.

- (U//FOUO) ***Rudimentary liquid diffusion:*** Many toxic chemicals at room temperature are either liquid or mixed with solvents to liquefy them. Terrorists could spread liquid chemicals on public items or places that people touch frequently. In addition, terrorists could puncture containers of toxic liquid within a confined area, allowing both dermal penetration and, as the chemical evaporates, respiratory absorption.
  - (U//FOUO) Aum Shinrikyo punctured an estimated 11 one-liter bags of liquid sarin on several subway cars in its 1995 attack on the Tokyo subway system. A U.S. medical doctor who investigated the attack speculated that if the sarin had been aerosolized, the number of casualties would have been far higher than the 12 deaths recorded.
- (U//FOUO) ***Dermal contact:*** Terrorists could place powder on objects people frequently contact, such as railings. Another method would be to introduce chemicals into a mail system, as was done in the U.S. anthrax attacks in 2001.

— (U//FOUO) ***Aerosol dispersal:*** Terrorists might use an aerosol-generating device to convert liquid chemical into a vapor cloud. The device could be initiated by a person in protective gear, by remote control, or by a suicide operative. Crop dusting airplanes and their pesticide aerosolizing devices could be used on a large scale; and simpler, commercially available foggers or sprayers would be effective on a smaller scale.

— (U//FOUO) ***Injection:*** Terrorists could inject a chemical directly into the bloodstream of an individual.

— (U//FOUO) ***Use of an explosion to deliver an agent:*** Terrorists could create an explosive device to disperse the chemical agent upon detonation; militaries use similar methods to disperse warfare agents. The effectiveness of such a delivery depends on the amount of agent that survives the heat and pressure of the blast and the meteorological conditions.

  – (U//FOUO) In 2004, Iraqi insurgents exploded a device improvised from a 155mm artillery shell that contained degraded sarin. The attack failed to inflict casualties, but two U.S. service members were treated for minor symptoms usually associated with the agent.

(U) Process Control Systems

(U//FOUO) Control systems such as SCADA, process control systems, and distributed control systems are used widely in the chemical, electric power, natural gas and oil, telecommunications, transportation, and water sectors. Cyber exploitation of hardware or software vulnerabilities could impair the functioning of control systems, disrupt or degrade service, and possibly damage other infrastructure components.

(U) Cyber Attack

(U//FOUO) Severe cyber attacks could disrupt, deny, destroy, or allow hackers to exploit systems and networks essential to the functioning of critical U.S. infrastructure with potentially devastating effects on economic security, the environment, national security, and public health and safety. For example, attacks on control systems (Supervisory Control and Data Acquisition [SCADA] or process control) could disrupt electric power distribution or cause the loss of control of chemical processes. Other examples include creating confusion or panic by degrading Internet traffic to such a degree that critical sites become inaccessible.

(U) Definition

(U//FOUO) A cyber attack comprises the actions taken through computer networks to disrupt, deny, degrade, destroy, or manipulate information in computers or computer networks, or the computers or networks themselves. This attack method can be used to

target cyber infrastructure that, as defined in the National Infrastructure Protection Plan, includes electronic information and communications systems and the information contained in those systems. Computer systems, control systems (SCADA), and networks—such as the Internet—are part of cyber infrastructure.

(U//FOUO) Cyber attacks occur in directed and nondirected forms. Directed attacks target specific computer systems or networks or use those systems or networks to attack other targets. Nondirected attacks are not targeted at a particular entity or sector, but can cause widespread disruptions to systems and networks. Both directed and nondirected attacks can degrade availability of critical cyber infrastructure and information, confidentiality, or integrity. They also can manipulate or cause malfunctions in critical infrastructure that rely on computerized control systems.

(U) Background

(U//FOUO) The increasing reliance on cyber infrastructure makes cyber attacks potentially attractive for adversaries (terrorists, criminals, foreign intelligence services, or corporate competitors) who wish to harm U.S. interests and cause mass disruption. Typical cyber infrastructure systems include business systems used to manage or support common business processes and operations; control systems that monitor and control sensitive processes and physical functions (chemical processing, electricity generation and distribution, and natural gas and oil production), and other specialty systems—such as safety, security, and support systems.

(U) Key Components

(U//FOUO) The key components of a cyber attack are a vulnerable target and a capable attacker with intent. Attackers may have the technical capability to understand the characteristics and vulnerabilities of the systems they are targeting and knowledge and expertise in cyber attack methods, they may make use of freely available tools that enable them to take action without an in-depth knowledge of architecture, configuration, or design, or they may partner with other like-minded or willing actors who possess the missing skills or knowledge.

(U//FOUO) **General Vulnerabilities:** Vulnerabilities can exist within a spectrum of targets in the cyber infrastructure. The increasing connectivity and integration of cyber systems, many of which can enhance business interoperability and reduce costs, can create multiple cyber points of entry that, if penetrated, would allow an attacker to extract proprietary or operational information or manipulate system controls to disrupt or degrade performance. For example, control systems are now frequently implemented with open connectivity (with remote access, and through business networks with subsequent connections to the Internet) and are potentially more vulnerable to various cyber attacks.

(U//FOUO) Security experts discover and report numerous hardware and software flaws daily. According to a major information technology security firm that tracks vulnerabilities, the release of patches for known vulnerabilities may lag days or months, leaving information and control systems vulnerable in the absence of effective protective measures.

(U//FOUO) **Capable attacker:** An attacker must have the intent and capability to conduct the attack. Individuals and small groups—generally motivated by money, politics, religion, or self-gratification—routinely conduct attacks against the U.S. cyber infrastructure. Islamic terrorist groups such as al-Qa'ida, HAMAS, and Hizballah have a growing appreciation of information technology to support their operations, and could parlay their cyber knowledge into attacks on U.S.-based information infrastructure. These organizations have expressed interest in capabilities that could exploit cyber vulnerabilities to disrupt provision of services, exact economic costs, and undermine public confidence. Terrorists also have the option of hiring hackers or organized criminal groups to launch attacks.

— (U//FOUO) In October 2005, British authorities arrested well-known cyber terrorist Younis Tsouli, known as Irhabi 007 ("terrorist 007"). Tsouli taught hacking techniques and discovered server vulnerabilities. He demonstrated his expertise by hacking a website run by a U.S. State Government and a U.S. academic institution. Tsouli maintained contacts with jihadists worldwide, possibly in the United States, the Bahamas, Sweden, and Tunisia, and including Bosnia, Canada, Denmark, Iraq, and the United Kingdom.

— (U) In 2005, an organization that tracks terrorist activity reported that a known jihadist website had posted an extensive beginner's guide to hacking websites and countering network security. The guide detailed methods on how to penetrate computer security and locate target computers and information on popular programs used to penetrate security.

(U) Potential Targets

(U//FOUO) The complexity of computing and communications systems in use in CIKRs coupled with their dependencies on those systems can create a number of possible options in attacking cyber infrastructure. Attacks could be directed at the control systems themselves, attacks on data or data processes, or attacks on the network communications mechanisms and networks.

(U//FOUO) **Attacks directed at control systems:** Attackers could exploit the computer control systems used to automate industrial processes and to generate and distribute power, manage transportation systems, treat water, and manage or deliver other critical infrastructure functions. Sophisticated attackers may attempt to gain access to an infrastructure asset's computer control system to create economic disruption, hazardous

conditions, or general mischief and specific terror. Attackers have gained access to control networks through connections to business management networks that were connected to the Internet. They also have exploited default vendor configurations on hardware and software. The effects are dependent on the type of operation controlled by the particular control system and the access level attained by the attacker. To cause specific types of effects, the attacker must be familiar with the network protocols and the configuration of the system. Many of these systems are in use globally, thus making their architectures, protocols, and default configurations broadly available. However, specific implementations can be highly sophisticated and difficult to understand. Even without in-depth knowledge, an attacker using basic methods could cause random failures or widespread disruptions.

(U//FOUO) **Attacks on data or data processes:** The information contained in a computer system is a vital asset to the business owner. The information asset owner must be able to trust the data's availability, confidentiality, and integrity. By simply gaining access to a data set, an adversary has successfully attacked the confidentiality of information. In addition, trust in the data's integrity is degraded, and the asset owner can no longer be sure that data are accurate and reliable. Finally, an intruder with access to a data set can prevent the information owner's access to it. Attackers have stolen and sold data, and they have extorted money from information owners by holding systems hostage (by encrypting data until ransom is paid).

(U//FOUO) Attackers can inject modifications to database application software or inject incorrect data, causing the systems to perform unpredictably. The injections could use physical media such as a compact disk or a Universal Serial Bus drive (flash, stick, or thumb drives), or use a data transfer that occurs over a network. Possible effects include erratic or incorrect performance, physical damage to the operations or facility, or the system ceasing to communicate. If this is done stealthily over an extended time, backups could also be affected, resulting in loss of confidence in restoration processes and causing the information owner to have to rebuild databases from scratch—an extremely expensive and time-consuming process.

(U//FOUO) **Attacks on the network communications mechanisms and networks:** The cyber attack methods used to compromise communications and computer networks are as diverse as the targets at which they are aimed. Attacks that affect the Internet either by directed or nondirected means can impede the ability of an infrastructure asset to function properly. Some attacks include packet crafting, in which specially crafted data packets are placed on a network to exploit vulnerabilities in applications, allowing the attacker access to the computer or network. In addition, an attacker can use a number of tools and techniques to gain access to a computer or network through broadband connections, wireless access points, and modems. Consequences include denial of service, which can deprive access by users to network resources and exploitation of data as detailed above.

(U//FOUO) Methods of Employment

(U//FOUO) **Use of malicious software:** Malicious software (malware) is software designed to infiltrate or damage or use the resources of a computer system without the owner's consent. Attackers use malware to obtain unauthorized access to information, alter information, or damage the targeted system or network. Common types of malware include Trojan horses, viruses, and worms—often delivered through the use of botnets. Unauthorized access to a system or network enables attackers with malicious intent to view, copy, change, or delete any data contained on the system. The damage an attacker can inflict depends on the level of access gained. Once malicious code has infected a system, the attacker can then run rootkits to obtain higher levels of access and install "backdoors" to gain future access covertly, potentially appearing as an authorized user. Malware also may exploit the compromised system's resources to gain access to the systems of trusted partners who use the network.

(U//FOUO) **Denial-of-Service attacks:** A Denial-of-Service (DoS) attack denies or impairs the authorized use of applications, networks, or systems by preventing access or exhausting resources. The three most common types of DoS attack are consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, and physical destruction or alteration of network components. The most common DoS attack involves dispatch of malformed packets (units of data routed over a network) or large volumes of packets. A single malformed packet can be used to cause a DoS; however, to generate the necessary volume of attack traffic to overwhelm a site, attackers typically use a distributed network of compromised hosts (botnet).

(U//FOUO) **Botnets:** A "bot," short for robot, is an automated software program that can execute certain commands. A botnet is an aggregation of compromised computers or bots that are connected to a central controller. Botnet operators typically offer a variety of malicious services, including anonymous proxy services, Distributed Denial-of-Service (DDoS) attacks, spam-for-hire, and others by issuing instructions to one or more botnets under their control. Botnets also serve as a focal point for collecting confidential and personally identifiable information from unsuspecting bot-infected systems. Botnets are available for sale or lease over the Internet, and versions controlling tens of thousands of compromised hosts are not uncommon. Botnets have grown in size and complexity in recent years and may fuel an underground economy in which compromised systems, credit cards, pirated media, personal information, and software license keys are bought and traded. Over the past several years, attackers have shifted their focus away from performing random DDoS attacks to generating revenue for their operators.

(U//FOUO) **Social engineering:** Attackers are increasingly using social engineering techniques to gain key information about the target that they can subsequently use to gain access to the target's computer or network. Some of the research methods involve simple telephone calls or elaborate e-mail ruses to elicit information or open an exploitable vulnerability (referred to as phishing). Other methods include accessing public financial records, dumpster diving, Google Hacking, requesting sunshine law information, sending

phony e-mails, and Who Is lookups (a means for finding or identifying an individual's or organization's Internet address).

(U) Food or Water Contamination

(U//FOUO) Chemical, biological, or radiological agents may be used to contaminate food or drinking water systems with the intent to cause economic disruption, generate public anxiety, or injure or kill people. U.S. food and water systems are vulnerable to contamination, and terrorist groups have expressed interest in carrying out such attacks.

(U) Definition

(U//FOUO) Agents potentially available to contaminate food or water systems include the following:

— (U//FOUO) **Chemical:** arsenic, benzene, cyanide, dioxin, lead, mercury, pesticides, and thallium.

— (U//FOUO) **Biological:** *Bacillus anthracis* (anthrax), *Clostridium botulinum* toxin, *Cryptosporidium parvum,* and *Salmonella typhimurium*.

— (U//FOUO) **Radiological:** high-level radioactive waste from the reprocessing of spent nuclear fuel (although the radiation from these materials would be sufficient to kill within a relatively short time, handlers would require specialized robotic equipment and significant amounts of shielding); low-level radioactive waste, generally in the form of radioactively contaminated industrial or research waste; naturally occurring radioactive material; transuranic radioactive waste from manufacture of nuclear weapons; and uranium mill tailings from the mining and milling of uranium ore.

(U) Background

(U) Food Systems

(U//FOUO) The U.S. food system is vulnerable to diseases, pests, and toxic materials that occur naturally or are introduced either deliberately or unintentionally. The system is complex, diverse, extensive, interconnected, and open, providing many potential targets for terrorist attacks. A successful attack on the U.S. food system could have severe economic and health effects.

— (U//FOUO) The mujahidin poisons handbook has been available on the Internet for several years. The handbook includes instructions for preparing and using several effective food contaminants such as nicotine and botulinum toxin. Many Islamic extremist groups posted this popular handbook on their websites, indicating an interest in these poisons.

— (U//FOUO) Around 2003, Islamic extremists in the United Kingdom discussed the possibility of using a syringe to inject poison into containers of beer at soccer games, but did not follow through.

(U) Drinking Water Systems

(U//FOUO) The accessibility and vulnerability of associated infrastructure, the availability of open source information on drinking water systems, and the potentially significant economic and public health consequences of a contamination attack make drinking water systems a possible terrorist target. Except for closed water systems or systems serving small communities (such as buildings or neighborhoods), dilution and chlorination can limit the effectiveness of water contamination as a terrorist tactic.

(U//FOUO) Transnational terrorists such as al-Qa'ida and affiliated groups pose a threat to the water sector, given their stated intent and potential capability to contaminate or sabotage water systems.

— (U//FOUO) A fatwa (a legal opinion or ruling issued by an Islamic scholar) posted on an Islamic website in May 2003 included justifications for the poisoning or disruption of U.S. water supplies. Near that time, Abu Mohammed al-Ablaj, a prominent Saudi cleric, e-mailed the London-based Arabic magazine, *Al-Majallah,* a message stating that al-Qa'ida would not rule out "poisoning drinking water in U.S. and Western cities."

(U) Key Components

(U//FOUO) To contaminate U.S. food production and drinking water systems, terrorists must obtain a contaminant and the means to disperse it to the intended targets. U.S. food industries include not just production, but also transportation, processing, packaging, distribution, retail and wholesale outlets, restaurants, and marketing. Where contamination occurs along the pathway from manufacture to consumer determines how many consumers are affected. Chemical, biological, and radiological contaminants, as well as equipment needed to disperse agents, could be bought, fabricated, or stolen.

(U) Food Systems

(U//FOUO) The chemicals used to contaminate a food system include toxic industrial chemicals (TICs) and chemical warfare agents. TICs are widely available and can be purchased or stolen. The use of a TIC bypasses the difficulties associated with obtaining a chemical agent, most of which would need to be synthesized in a laboratory. Some information describing the production of chemical agents is publicly available, but these "recipes" often are flawed and likely would require an individual with graduate-level chemistry education or an equivalent amount of laboratory experience to properly execute the procedures and recognize any incorrect synthesis information. Production

equipment and precursors for chemical agents generally can be obtained from commercial sources.

(U//FOUO) The ability to obtain the pathogen involves either isolating an organism from the environment, obtaining it from a state program or acquiring it from a laboratory culture collection. In marked contrast to chemical agents, most biological agents can be obtained from natural sources, although natural strains vary widely in their virulence. Regardless of how the pathogen is obtained, the terrorists almost certainly will use an animal to determine the pathogen's virulence.

(U) Drinking Water Systems

(U//FOUO) A biological attack against drinking water systems may be easier for potential adversaries than other attack methods since it may not involve complex steps to weaponize an agent. In large public water systems, however, dilution, filtration, and chlorination will limit the impact of biological agents. Toxic industrial chemicals are readily available and relatively simple to store, transport, and introduce into the drinking water supply. A successful attack on a drinking water system would require detailed knowledge of the water distribution system unless directed against a select few targets.

(U) Methods of Employment

(U) Food Systems

(U//FOUO) **Contamination of food imports:** According to U.S. Department of Agriculture (USDA) Economic Research Service estimates, imported food accounts for 11 percent of the food consumed in the United States. Terrorists may seize the opportunity to contaminate imported food during production, storage, or transportation where access to food may be more readily available and detection less likely. This attack method would require knowledge of which contaminants would remain effective through processing and transport, as well as knowledge of the destination of the product.

- (U//FOUO) In 1978, a Palestinian group called the Arab Revolutionary Army claimed it injected oranges exported from Israel with mercury to sow panic and wreck the country's economy. Five Dutch children fell ill, and European officials checked thousands of oranges.

(U//FOUO) **Contamination of food during processing:** Ingredients used in food processing come from many sources both domestic and foreign. When these ingredients are processed in large batches and often uniformly mixed, chemical, biological, and radiological contaminants could be introduced and rapidly and widely distributed throughout the food supply.

(U//FOUO) **Contamination of food during transport:** In January 2005, the American Transportation Research Institute released a USDA-funded report on food transit security

that reported a leading concern among survey respondents was security at rest stops and parking areas. Some carriers, especially those using a higher percentage of contracted drivers, also labeled personnel issues as a major concern. Weaknesses in rest stop and personnel security provide openings for the deliberate contamination of food products. Contamination at these points in the supply chain could be difficult to trace or attribute.

— (U//FOUO) In April 2005, DHS/Customs and Border Protection reported the interdiction at a northern border port of entry of a Canadian citizen with a commercial driver's license who was watch listed for terrorist connections. The individual was transporting a shipment of pasta into the United States. No evidence existed of terrorist-related activity, but this incident demonstrates the ease of access to the U.S. food supply by high-risk individuals.

(U//FOUO) **Contamination of food during distribution:** The Nation's 13,000 convenience stores, 28,000 gas station food outlets, 13,000 smaller food markets, 34,000 supermarkets, and 1,000 wholesale club stores provide numerous venues and opportunities for terrorists to contaminate the food supply. At the distribution stage, however, most food products are in consumer-ready or individual serving-size packages, making it difficult to effectively contaminate large amounts of food.

— (U//FOUO) In April 1946, a vengeance group called Nakam gained access to a bakery that supplied bread to Nazi soldiers interred in a prison camp in Nuremberg. Members of the group coated 3,000 loaves of bread with arsenic. Reportedly thousands of prisoners suffered severe stomachache, and hundreds were admitted to the hospital for medical attention, but no one died.

— (U//FOUO) In 1984, members of the Rajneesh religious cult attempted to influence a local election in Oregon by infecting salad bars with *Salmonella typhimurium* in 10 area restaurants, infecting 751 people. This incident was the first known 20th century biological attack in the United States.

(U) Drinking Water Systems

(U//FOUO) **Contamination of raw water sources (lakes, reservoirs, rivers, and wells) prior to treatment:** Contaminants could be introduced at various points along the transmission line, particularly if aqueducts are open or conduits are above ground and easily accessible. Contaminants also may be pumped directly into the raw water sources prior to transportation or at treatment plant intakes. Water quality monitoring by local water authorities and the effects of fluorination/chlorination and the filtering of surface waters can limit the effects of a potential contaminant.

— (U//FOUO) In 1972, members of the cult, "Order of the Rising Sun," were arrested with more than 30 kilograms of typhoid cultures they intended to use in poisoning water supplies in Chicago, St. Louis, and other American cities.

(U//FOUO) **Contamination of distribution systems or water storage tanks following treatment:** Contaminants could be pumped directly into aboveground storage tanks or uncovered storage reservoirs. A contaminant also could be introduced into a drinking water distribution system using access points such as fire hydrants and most types of commercial and residential connections.

— (U//FOUO) In 2002, Italian police arrested four Moroccan nationals for allegedly plotting a chemical terrorist attack on U.S. Embassy Rome. The suspects had approximately 9 pounds of potassium ferrocyanide and maps detailing the location of the water pipes that serve the Embassy. Police discovered an underground passageway next to the Embassy large enough for someone to crawl through and reach the pipes.

— (U//FOUO) The U.S. Environmental Protection Agency conducted a tracer study in an urban residential district in which authorities were aware of the study but residents were not. Technicians in unmarked vehicles pumped a food-grade substance bought at a local hardware store through a fire hydrant connection for more than eight hours without arousing residents' suspicion. This example demonstrates the ease with which contaminants could be introduced into a drinking water distribution system.

(U//FOUO) **Backflow contamination:** Contaminants could be pumped back into the water system through output sources such as restroom sinks, toilets, or water tanks, potentially contaminating the water system in a localized area.

(U//FOUO) **Disabling or sabotaging the drinking water system:** Terrorists could increase the effect of contaminants by tampering with or disabling treatment equipment through cyber or physical attacks. If equipment is disrupted and raw water is not properly treated, contaminants introduced into a water source could continue through the finished water storage tanks and into the distribution system.

(U) Hostage Taking

(U//FOUO) Terrorists could take hostages to gain control of a CIKR. This method of attack has never been employed by international terrorists in the United States, but virtually every U.S. critical infrastructure sector has facilities that could be vulnerable to this method of attack.

(U) Definition

(U//FOUO) Hostage taking is the seizure or detention of a person with the threat to injure, kill, or continue to detain to compel a third person or governmental organization to do, or to abstain from doing, an act as a condition for the person's release. Terrorists could take hostages for gaining control of or sabotaging CIKRs.

(U) Background

(U//FOUO) Terrorists and other elements have used hostage taking throughout history, traditionally as a means of achieving ideological, monetary, or political gain. Terrorists also could use this method of attack to gain access to critical infrastructure operations and, in some cases, use the access to launch additional attacks.

— (U) In June 2006, the Canadian Government uncovered an alleged terrorist plot to storm the Ottawa Parliament, hold politicians hostage, and demand the release of Muslim prisoners from Canadian jails and the withdrawal of Canadian military forces from Afghanistan.

— (U) In 2004, Chechen terrorists took more than 1,200 school children and teachers hostage in a school in Beslan, Russia. The terrorists hung bombs from the basketball nets and beams of the school gymnasium where the hostages were held and demanded Russia withdraw its military from Chechnya. On the third day of the standoff, gunfire broke out between the hostage takers and Russian security forces, killing at least 330 civilians, including 156 children, and wounding hundreds more.

— (U) Rebels from the 30th Front of the Revolutionary Armed Forces of Colombia (FARC) held more than 100 employees and journalists hostage at the Alto Anchicaya hydroelectric plant in Dagua on 31 August 1999. They requested a report on the "social impact the dam has had in favor of customers" and demanded a 30 percent cut in energy fares. All the hostages were released unharmed by 5 September 1999.

(U) Key Components

(U//FOUO) Different organizations maintain a variety of guidelines for hostage taking. Al-Qa'ida sets forth the following requirements in its training manual, *Al-Battar:*

— (U) Capability to endure difficult circumstances and psychological pressure. In the case of a public kidnapping, the team will be under a lot of pressure.

— (U) Intelligence and quick reflexes to deal with an emergency.

— (U) Capability to take control over the adversary.

— (U) Good physical fitness and fighting skills.

— (U) Awareness of the security requirements prior to, during, and after the operation.

— (U) Ability to use all types of light weapons for hostage taking.

(U) Methods of Employment

(U//FOUO) **Mass hostage taking event:** This method involves a number of terrorists, typically with improvised explosive devices or small arms weapons, detaining a large group of people regardless of demographic distinctions, using threats of harm and issuing demands. Terrorists typically make political or monetary demands, such as the release of fellow terrorists from government custody, often threatening to kill or otherwise harm hostages if the demands are not met. Terrorists could use antiintrusion munitions or suicide vests to deter a local security force intervention. This scenario may require more coordination and equipment than smaller scale attacks.

— (U//FOUO) The al-Qa'ida training manual assumes hostage taking will be conducted by large groups of operatives, dividing them into three subgroups: the guarding and control group, whose role is to seize control of the hostages and get rid of them in case the operation fails; the protecting group, whose role is to protect the abductors; and the negotiating group.

— (U//FOUO) In October 2002, Chechen terrorists took more than 800 patrons hostage in a Moscow theater. The explosives-laden terrorists demanded that Russia withdraw its troops from Chechnya. At least 50 terrorists and more than 90 of the hostages were killed during the three-day siege, which ended when Russian Special Forces stormed the theater.

— (U//FOUO) The largest hostage taking of diplomats occurred on 27 February 1980 when 16 terrorists from the 19th of April (M–19) group assaulted Dominican Republic Embassy in Bogota, Colombia. Armed with shotguns and small arms, they seized 60 diplomats (including the U.S. Ambassador to Colombia), Colombian officials, guests, and local employees. They demanded $50 million from the countries whose diplomats were held and the release of 311 jailed comrades. Their demands were rejected, and after 61 days they reached a compromise with the Colombian Government. The terrorists flew to Cuba with several of the hostages, who were released upon landing. The terrorists themselves were allowed to remain in Cuba.

(U//FOUO) **Targeted hostage taking:** In this attack method, terrorists target specific groups of hostages, such as by age, ethnicity, geography, group association, national origin, or religion.

— (U//FOUO) In December 1996, members of the Tupac Amaru Revolutionary Movement entered the residence of the Japanese ambassador to Peru during a party and took diplomats, business executives, and government and military officials hostage. The terrorists threatened to kill the hostages if their imprisoned comrades were not released from Peruvian jails. Four months after the hostage taking, Peruvian soldiers stormed the ambassador's residence, killing all 14

terrorists. The soldiers rescued 72 hostages, although one Japanese hostage and two soldiers were killed.

(U//FOUO) **Conducting a hostage-taking to seize a critical infrastructure asset or system:** Terrorists could use this method to gain control of a facility to sabotage its operations or initiate a larger attack. Terrorists may attempt to coerce facility operators to conduct operations that could harm people or infrastructure assets. Terrorists also may have enough detailed knowledge of the facility's functions and layout to adjust the operations to meet their goals.

— (U) In May 2000, a group of FARC rebels armed with gas tanks seized the La Salvajina hydroelectric plant in Suarez, Colombia, leaving the area without power for approximately 10 hours. After subduing the four operators and a security guard, the terrorists entered the facilities and stayed there for more than two hours. No damage was reported to the facility. The FARC claimed the company in charge of the plant had not fulfilled agreements signed with the terrorist group the year before.

(U) Improvised Explosive Device

(U//FOUO) Improvised explosive device (IED) attacks are the favored method of most terrorist groups around the world. Trends in IED employment indicate terrorists continue to pursue and exploit ways to maximize the effects of this kind of attack. CIKRs are a common target for IED attacks, which have the potential to cause significant consequences.

(U) Definition

(U//FOUO) An IED is an explosive device that is fabricated in an improvised manner from explosives, or other destructive, incendiary, lethal, or pyrotechnic materials and chemicals. IED design is limited only by the ingenuity of the bomber and the materials that are available. IEDs may be concealed within containers that disguise their presence. They have been concealed artfully within objects as varied as books, cargo, portable radios, shoes, and toys, among other things. (Vehicle-borne improvised explosive devices are addressed as a separate attack method.)

(U) Background

(U//FOUO) IEDs have been used extensively in warfare to attack facilities and security barriers and to inflict civilian and military casualties. Documented instances indicate their use during the Vietnam War and World War II. The Irish Republican Army and other groups in Northern Ireland used IEDs extensively in their campaign against the British Army. More recently, insurgents in Iraq have become adept at producing, concealing, and employing IEDs. Between May 2003 and May 2004, more than

15,000 IED attacks were reported in Iraq, accounting for more than 50 percent of Coalition casualties. Iraqi insurgents have gained most of their IED experience and knowledge by firsthand experience or training, but they also have benefited from information and tactics developed by insurgents or terrorists in Bosnia, Chechnya, and Israel, which are readily available on the Internet and other media.

(U//FOUO) Terrorist groups have favored IEDs as a tactic for targeting people at critical infrastructure venues. Attacks against mass transit systems in London, Madrid, and Mumbai have demonstrated the lethality of IEDs.

(U) Underwater Threats Using IEDs

(U//FOUO) IEDs also could be used in underwater tactics against CIKRs. Possible targets could include the following: attraction and entertainment venues; channels, chokepoints, dams, and locks; military targets; nuclear power plants; chemical and oil facilities; transportation targets; water treatment facilities; and vessels (anchored, moored, or under way).

(U//FOUO) Swimmers (placed or suicide). Swimmers, including those aided by submersible devices, could place or detonate an explosive device under water—at, near, or on a target.

(U//FOUO) Mines (and mine-like devices). A drifting mine or a bottom, buried, moored mine, or self-propelled explosive (such as torpedoes) could impact facilities or vessels.

(U//FOUO) Underwater unmanned device. Explosives could be delivered to targets underwater by a commercial submersible device.

(U//FOUO) Parasitic attachment. A parasitic attachment containing explosives could be placed on a target.

(U) Key Components

(U//FOUO) U.S. and Coalition military forces in Afghanistan and Iraq have witnessed increases in the sophistication and use of IEDs against civilian and military targets. IEDs vary widely in design features and shape, but most share four basic elements: power supply, initiator, explosives, and switch or sensor. Some IEDs use mechanical mechanisms or pyrotechnics instead of an electric power source, such as the case with Richard Reid's shoe bomb.

(U//FOUO) The effectiveness of an IED does not depend solely on the amount of explosives. Each element of a device can be tailored specifically to suit the attack scenario. Each element can be crude or sophisticated, depending upon the attack environment, the requirements, resources, and skill of the bombmaker.

— (U//FOUO) Devices have been hidden in inconspicuous items and places, such as animal carcasses, guardrails, plastic bags, and trash. Insurgents in Iraq have used

commercially manufactured explosives, homemade explosives, and military ordnance as the main explosive charge in their IEDs.

(U//FOUO) When an IED detonation occurs, three effects cause casualties and destruction: blast, fragmentation, and thermal.

— (U//FOUO) **Blast:** The blast is caused by overpressure resulting from a near-instantaneous conversion of solid or liquid explosives into rapidly expanding hot gases. The blast and can knock down buildings and propel objects and people great distances.

— (U//FOUO) **Fragmentation:** Terrorists may choose to include materials that, upon detonation, will generate high-velocity fragmentation. Alternatively, they may choose to detonate an IED close to materials anticipated to cause additional or collateral damage. Fragmentation is typically categorized as primary or secondary. Primary fragmentation consists of shattered pieces of the explosive device, sometimes referred to as "shrapnel." Fragmentation also can result from the deliberate inclusion of objects such as ball bearings, nails, or other hardware into the design of the IED. Such objects can be externally affixed or mixed with an explosive filler, and are sufficiently strong to survive the blast and to puncture skin when propelled by force. Secondary fragmentation is nearby debris propelled by the blast, but at a lower velocity than primary fragmentation.

— (U//FOUO) **Thermal:** The thermal effect contributes relatively little compared with the damage from the destructive force, since the fireball generally will not exceed the blast radius.

(U) Methods of Employment

(U//FOUO) In the past few years, terrorists have employed increasingly sophisticated tactics in conducting IED attacks. Tactics include greater frequency of simultaneous or coordinated multiple bombings; small arms fire and indirect fire with IED attacks; and increased use of secondary devices that channel intended victims to locations where a second device targets first responders, onlookers, and those fleeing an initial attack.

— (U//FOUO) On 12 October 2002, Jemaah Islamiya (JI) operatives used an IED attack by a suicide bomber to funnel potential victims into crowded streets in a popular tourist area in Bali, Indonesia. Shortly afterward, terrorists detonated remotely a second, much more powerful IED concealed in a van, causing most of the fatalities.

(U//FOUO) IED employment methods are numerous, but two of the most common tactics terrorists use are delivery and detonation by suicide bombers and placement of a device at a target for subsequent detonation.

(U//FOUO) **IEDs carried by suicide bomber:** Terrorists often employ a suicide bomber who typically carries a concealed explosive device to the target and detonates it with full expectation of dying in the attack. The terrorist may carry the device in something as simple as an athletic bag or attempt to conceal it in a belt or vest. Suicide bombing often is successful because the devices can be simple in design and allow flexibility (adaptation and improvisation) during execution of the attack, making it difficult to detect and prevent. This attack method can employ a single bomber or multiple operatives working simultaneously or in a staggered pattern. This method has the potential to inflict harm on a large number of individuals and to increase the likelihood of psychological impact on the general public.

(U//FOUO) Suicide attacks often present a favorable cost-and-effect ratio to insurgents. This has led to a steady expansion in the use of suicide bombers. Insurgents conducted more than 400 suicide bombings in Iraq between the Coalition invasion in 2003 and July 2005.

— (U//FOUO) The number of female suicide bombers has increased. Al-Qa'ida is recruiting female jihadists and suicide bombers in Iraq and abroad. Female suicide bombers have used suicide belts or vests and also have strapped large amounts of explosives to their stomachs, allowing them to operate under the guise of pregnancy.

— (U) In August 2006, UK authorities disrupted a terrorist plot to smuggle liquid components of an explosive on board several aircraft, assemble full devices in flight, and detonate them en route from the United Kingdom to the United States.

— (U//FOUO) In 2005, suicide bombers detonated three bombs within one minute of each other on different London subway cars. A fourth terrorist's device detonated on a London bus. All four terrorists were killed, as were 52 other persons, and 700 persons were wounded.

— (U//FOUO) In 2001, Richard Reid, a British Islamic fundamentalist and alleged al-Qa'ida operative, attempted unsuccessfully to ignite the fuse for the device packed in his shoes during a flight from Paris to Miami.

(U//FOUO) **Placed IEDs:** Static or placed IEDs may require more time and planning, which can limit flexibility in executing an attack. Remotely detonated IEDs, however, can provide obvious physical safety for a terrorist.

— (U//FOUO) On 11 July 2006, terrorists set off seven blasts over 11 minutes on the Suburban Railway in Mumbai, India. The attacks killed 209 people and injured more than 700.

— (U//FOUO) On 11 March 2004, terrorists remotely detonated 10 IEDs with a dynamite main charge on the Madrid train system, killing nearly 200 people and wounding more than 1,400.

(U) Maritime Vessel as a Weapon

(U//FOUO) Terrorists have used maritime vessels as weapons successfully in attacks overseas and could conduct similar attacks against critical infrastructure targets in the United States. The use of a small boat as a weapon is likely to remain al-Qa'ida's weapon of choice in the maritime environment, given its ease in arming and deploying, low cost, and record of success.

(U) Definition

(U//FOUO) Maritime vessels include the following: fuel tenders (bunker barges); pleasure craft of all types; specialized surface and sub-surface craft; submarines; tugboats; and vessels used in cargo transport, commercial fishing, and passenger transport (including cruise vessels and ferries).

(U//FOUO) Terrorist use of a maritime vessel as a weapon is one of several attack methods that may be employed under maritime terrorism. This attack method involves using a vessel to undertake terrorist acts and activities within the maritime environment; against other vessels or fixed platforms at sea or in port or their crews and passengers; and against coastal facilities or settlements, including cities, port areas, port towns, cities, and tourist resorts. In the United States, inland facilities such as those along the Great Lakes also are possible targets.

(U) Background

(U//FOUO) The maritime sector encompasses a broad array of potential targets, such as cargo and passenger terminals, passenger ferries and their terminals, gas and oil infrastructure, and locks and dams, waterways, and vessels. Certain international terrorist organizations, among them the Sea Tigers of the Liberation Tigers of Tamil Eelam and al-Qa'ida, have demonstrated well-developed maritime attack capabilities outside the United States.

(U//FOUO) Attacks on USS *Cole* in October 2000, the French supertanker M/V *Limburg* in October 2002, and maritime vessel suicide attacks against Iraqi oil terminals in April 2004 demonstrate that U.S. maritime assets are at risk to terrorist attacks using maritime vessels as weapons.

(U) Key Components

(U//FOUO) Several key elements are necessary for terrorists to conduct an attack using a maritime vessel as a weapon. These include the ability to hijack, purchase, or steal a vessel; the ability either to pilot or to dictate the piloting of the vessel to the intended target; knowledge of and ability to create and use explosives (when used) with sufficient power to cause damage to the target; and the ability to use deception rather than speed to gain target access when using larger vessels such as fishing trawlers.

(U) Methods of Attack

(U//FOUO) When using a maritime vessel as a weapon, terrorists may employ two primary methods: a vessel laden with explosives as a weapon, and the vessel itself as a weapon (kinetic attack). In using a large commercial vessel as a kinetic weapon, terrorists also can take advantage of the vessel's legitimate cargo, such as liquefied natural gas or petroleum, to enhance the destructive effects of an attack.

(U//FOUO) **Using vessel cargo as a weapon:** Al-Qa'ida's weapon of choice in maritime attacks has been the small, explosives-laden vessel, usually piloted by a suicide operative. Terrorists are likely to select a relatively small, nimble boat, or one that could approach a larger vessel without arousing suspicion, such as a fuel tender, harbor trader, tugboat, or other service vessel. Once the vessel is loaded with explosives, the terrorists maneuver it to the target and detonate the explosives. In the case of an unpowered vessel such as a barge, terrorists can wait for a moving target to approach its location and then detonate the explosives by remote control. This scenario assumes the adversary has the ability to conduct reconnaissance in the area of operations and the ability to develop and deploy an attack device in the desired location. Another tactic is to commandeer a patrol vessel or design one of similar appearance that can approach the target unmolested and unchallenged.

- (U//FOUO) On 24 April 2004, three fishing dhows (small traditional boats) attempted to attack the Al-Basrah Oil Terminal and the Khor al-Amaya Oil Terminal oil platforms off southern Iraq. When a Coalition team attempted to board the first dhow, it exploded, flipping the U.S. Navy craft and killing two U.S. Navy service members and one U.S. Coast Guard service member. The second dhow also exploded when approached by a security team. These attacks were attributed to al-Qa'ida.

- (U//FOUO) In October 2002, al-Qa'ida operatives attacked the French supertanker M/V *Limburg* as it transited between Bahrain and Yemen. A suicide attacker piloting a small dinghy loaded with several hundred pounds of TNT rammed the side of the tanker. One crewman was killed and 12 were injured; approximately 90,000 barrels of oil spilled into the Gulf of Aden.

— (U//FOUO) On 12 October 2000, al-Qa'ida operatives conducted a suicide attack against USS *Cole* in Aden harbor in Yemen. The terrorists packed between 400 and 700 pounds of C–4 plastic explosives around the frame of a small rubber boat powered by an outboard motor. They piloted the boat into the side of the warship and detonated the explosive, killing 17 U.S. Navy service members and wounding 39.

(U//FOUO) **Kinetic attacks:** This method of attack involves piloting a vessel into another vessel or coastal target. Terrorists most likely would need to hijack such a vessel either by boarding surreptitiously or by commandeering it at sea. Kinetic attacks also could involve a barge with dangerous cargo that is set loose from its moorings into a rapid river current in an inland waterway or during a large tidal movement. Animal protest groups have used kinetic attacks against illicit fishing and whaling vessels for more than 30 years.

— (U//FOUO) In 1979, the R/V *Sea Shepherd*, a ship belonging to a marine wildlife conservation group, chased the whaling ship F/V *Sierra* into the Port of Leixoes, Portugal. The captain of the R/V *Sea Shepherd* used his vessel to ram the F/V *Sierra* twice in the harbor, tearing the hull open to the waterline and forcing the ship to undergo an estimated $1 million in repairs.

(U) Nuclear Attack

(U//FOUO) The detonation of a nuclear yield producing device would cause mass fatalities and infrastructure damage from the heat and blast of the explosion and significant consequences from both the initial nuclear radiation and the subsequent radioactive fallout. In addition, the economic and psychological impacts from such an attack would be significant. The Federal Government has placed a high priority on preventing terrorist groups from acquiring nuclear weapons or developing an improvised nuclear device. If terrorists acquired a nuclear weapon or improvised nuclear device, and had the flexibility to choose a target, their most likely primary target would be a population center that includes banking, finance, or commercial districts, government facilities, or national icons and monuments. Large areas surrounding the primary target would be affected to some extent by the radioactive fallout from a nuclear attack.

(U) Definition

(U) A nuclear weapon is a device with explosive power resulting from the release of energy unleashed by the splitting of nuclei of a heavy chemical element, such as plutonium or uranium (fission), or by the fusing of nuclei from a light element, such as hydrogen (fusion). Fusion (thermonuclear) bombs can be significantly more powerful than fission bombs, but are at this point believed to be beyond the capability of terrorists to construct. This paper will focus on the fission bomb.

(U//FOUO) **Categories:** The types of nuclear weapons a terrorist may use fall into two general categories: illicitly acquired weapons produced by nation-states and improvised nuclear devices (INDs).

- (U//FOUO) Nuclear weapons produced by sovereign nations are designed, constructed, and usually tested using financial, manufacturing, and technical resources of the nation. The weapons of nation-states typically produce high yields with high reliability and designed for a delivery vehicle, such as an aircraft or missile. The weapon likely would be lighter and smaller than an IND.

- (U//FOUO) An IND would be a crude nuclear device built from the components of a stolen weapon or from scratch using nuclear material, with untested yield and reliability. The greatest obstacle terrorists face when attempting to build an IND is obtaining enough fissile material to create a nuclear explosion. Crude nuclear weapons typically are heavy, ranging from a few hundred pounds to several tons. Specially designed small nuclear weapons, including the so-called suitcase nuclear weapons are much lighter, but they have never been acquired by terrorist organizations and are technically difficult to produce.

(U//FOUO) **Configurations:** Two basic nuclear weapon configurations exist. The first, called the gun assembly, incorporates two separate subcritical masses of fissile material that, when driven together by a propellant at detonation, form a supercritical mass resulting in an explosive fission chain reaction. The second, called an implosion system, uses a single subcritical mass of fissile material that compressed to a supercritical density by surrounding explosives to produce an explosive fission chain reaction.

- (U//FOUO) A gun-assembly weapon is the simplest type of nuclear weapon. Typically, chemical (explosive) propellant accelerates a subcritical fissile-material projectile down a gun barrel-like tube, where it meets with a subcritical fissile-material target to form a supercritical mass. A successful gun-type device would use highly enriched uranium (HEU). Little Boy, the 15-kiloton-yield weapon used at Hiroshima, was a gun-assembled device.

- (U//FOUO) An implosion weapon uses either plutonium or HEU. The need to achieve uniform spherical compression for the fission to take place makes an implosion device more difficult to design and build than a gun-assembly weapon. High explosives such as RDX or HMX compress the fissile material upon weapon initiation. One advantage of an implosion weapon is that less fissile material is required to produce a given yield compared with a gun-type weapon. Fat Man, the 21-kiloton-yield weapon used at Nagasaki, was an implosion weapon.

(U//FOUO) **Size of nuclear explosions:** Nuclear explosions are classified based on the amount of energy they produce, called yield. Given what we know of terrorist efforts, a terrorist nuclear weapon most likely would have a yield of less than 1 to several kilotons. A kiloton is the equivalent energy of 1,000 tons of TNT. Large military nuclear weapons

systems deliver weapons with yields in the multihundred kilotons to megaton (1 million ton) range.

(U//FOUO) **Effects of a detonation:** The effects of a nuclear detonation depend on the yield and success of the detonation. A low-yield (about 1 kiloton) device is one of the most likely weapons. Effects include air blast, heat, initial radiation, ground shock, and secondary radiation. The ground shock and air blast would cause major disruptions in the local infrastructure.

— (U//FOUO) ***Air blast:*** As with a conventional explosive, a nuclear detonation produces a shock wave, or air blast wave. The air blast from a 1 kiloton detonation could cause 50 percent mortality rate from flying glass shards to individuals within an approximate radius of 300 yards. This radius increases to approximately 0.3 mile for a 10 kiloton detonation.

— (U//FOUO) ***Heat:*** The second effect would be extreme heat, a fireball, with temperatures to millions of degrees. The heat from a 1 kiloton detonation could cause 50 percent mortality from thermal burns to individuals within an approximate 0.4 mile radius. The radius increases to approximately 1.1 miles for a 10 kiloton detonation.

— (U//FOUO) ***Initial radiation:*** The initial radiation is produced in the first minute following detonation. The initial radiation pulse from a 1 kiloton device could cause 50 percent mortality from radiation exposure within an approximate 0.5 mile radius, if individuals were not given immediate medical intervention. This radius increases to approximately 0.75 mile for a 10 kiloton detonation.

— (U//FOUO) ***Ground shock:*** Ground shock equivalent to a large localized earthquake also would occur. This could cause additional damage to buildings, communications, roads, utilities, and other portions of the infrastructure.

— (U//FOUO) ***Secondary radiation:*** Secondary radiation exposure from fallout would occur primarily downwind from the blast, but changing weather conditions could spread radioactivity and enlarge the affected area. For a 1 kiloton device, radiation exposure from fallout within the first hour after the blast could cause 50 percent mortality for approximately 3.5 miles downwind of the event. This distance increases to approximately 6 miles for a 10 kiloton detonation.

(U//FOUO) **Failed detonation or fizzle yield:** A fizzle yield occurs if the fissile material mechanically disassembles before a significant yield is generated. Even a fizzle yield, however, can produce a very large explosion that could disperse radioactive material widely, essentially becoming a radiological dispersal device or “dirty bomb.”

(U) Background

(U//FOUO) Usama Bin Ladin and al-Qa'ida have publicly expressed their clear desire to acquire weapons of mass destruction, including specifically nuclear weapons, to attack the United States. In a 1999 interview, Bin Ladin referred to acquiring biological, chemical, and nuclear weapons as a "religious duty." Since the late 2001 invasion of Afghanistan, U.S. and Coalition armed forces, and various members of the media, have recovered hundreds of documents detailing al-Qa'ida's quest to develop and use these weapons.

(U) Key Components

(U//FOUO) To conduct a nuclear attack on the Homeland, terrorists need possession of a nuclear weapon—created, purchased, or stolen—and the ability to deploy the weapon in the United States.

(U//FOUO) **Acquiring a weapon:** Terrorists possibly could acquire a nuclear weapon in several ways, including theft, purchase through illicit channels, or donation by a nuclear weapons capable state program. Generally speaking, nation states make every effort to secure weapons of this kind, which poses a formidable challenge to terrorists. Vulnerabilities may exist, however, in some countries that have nuclear weapons. Some weapons may have devices to prevent unauthorized use, or terrorists might lack confidence that they could make an acquired weapon work, but terrorists could deconstruct the weapon for nuclear materials and components to make their own device.

(U//FOUO) The manufacture of a nuclear weapon is a difficult challenge. The most difficult step is acquisition of a sufficient quantity of fissile material. Potential sources of fissile material include Russia and the countries of the former Soviet Union and nuclear research reactors throughout the world that may have inventories potentially at risk of diversion or theft. In addition to a source of nuclear material, a cadre of competent technical specialists would be required. Processing and machining of valuable and often dangerous materials are involved, requiring specialized equipment to cast and machine explosives, plutonium, or uranium.

(U//FOUO) **Deploying the weapon:** In addition to acquiring a nuclear weapon, terrorists must have the expertise to deploy the weapon, including transporting it into or within the United States and successfully detonating it.

(U) Methods of Employment

(U//FOUO) Several options exist for transporting a nuclear weapon into the United States. Once the weapon is inside the country, it could be moved by air, land, or sea. Potential methods to get the device into the country include the following:

— (U//FOUO) ***Use of aircraft*** flown from outside the United States, with the weapon either detonating in the air over a U.S. city or transferred to another mode of travel.

— (U//FOUO) ***Use of a container ship or oil tanker*** with detonation occurring in the port or transfer of the weapon to another mode of travel.

— (U//FOUO) Movement of the weapon by a ***smaller boat for infiltration*** to a populated coastal city for detonation or smuggling to less monitored coastal areas for transfer to another mode of travel.

— (U//FOUO) ***Transport by motor vehicle*** across a land border.

(U//FOUO) Five elements are common to these delivery scenarios:

— (U//FOUO) **Use of suicide teams:** Terrorist teams likely would be willing to conduct a suicide mission to ensure success and control of the weapon at all times.

— (U//FOUO) **Security focused:** Maintaining operations security and control of the weapon would be paramount, given the great expense, risk, and limited opportunities to attack with this method.

— (U//FOUO) **Target location:** Terrorists may focus on prominent economic, infrastructure, and political targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and fear among the U.S. population. A nuclear attack likely would be aimed at population centers situated along the periphery of the United States, since an attack at such locations would limit the logistics and risk of detection in transporting the weapon.

— (U//FOUO) **Points of entry:** Terrorists likely would attempt to bypass official ports and border crossings, particularly those known to conduct inspections or use detection equipment.

— (U//FOUO) **Backup planning:** If the mission is compromised before the weapon reaches its intended target, terrorists might detonate the nuclear device in place or at secondary targets rather than allow the plot to fail completely.

(U) Radiological Dispersal Device

(U//FOUO) Terrorists may consider a radiological dispersal device (RDD) as a useful weapon to cause panic and economic damage, although the lethality likely would be low. In a 1999 interview, Bin Ladin referred to acquiring nuclear, biological, and chemical weapons as a "religious duty." In addition, in September 2006 Abu Ayyub al-Masri, the

leader of al-Qa'ida in Iraq, called on scientists to come to Iraq to develop weapons of mass destruction, specifically "biological and dirty bombs."

(U) Definition

(U//FOUO) An RDD is any device that causes the purposeful dissemination of radioactive material without a nuclear detonation. Whereas a nuclear device uses radioactive material to create a nuclear fission or fusion explosion, RDDs use a material's natural radioactivity as a weapon. A dirty bomb is one type of RDD that uses a conventional explosion to disperse radioactive material over a targeted area. The term dirty bomb and RDD are often used interchangeably in technical literature, but RDDs also include other means of dispersal, such as placing a container of radioactive material in a public place or by aerosolization. A radiological exposure device (RED), also known as a radiation emission device, does not involve the active dispersal of radioactive material; instead, a radioactive source is placed in a location where it will expose nearby people to radiation.

(U//FOUO) It is difficult to design an RDD that would deliver radiation doses sufficient over a large enough area to cause immediate health effects or large numbers of fatalities. Most dirty bombs and other RDDs would have very localized effects, ranging from less than a city block to several square kilometers. In an explosive dispersal, the initial explosion likely would kill more people than the radioactivity, since the radiation levels following an attack generally would not be lethal or cause severe acute radiation sickness. The degree of contamination would depend on factors such as the area covered by the dispersal, the amount and type of radiological material used, and meteorological conditions.

(U) Background

(U//FOUO) An RDD attack has never occurred, but the effects can be estimated from calculations and comparisons to radiological accidents. In 1987, two scrap metal scavengers broke into an abandoned radiotherapy clinic in Goiania, Brazil and removed a sealed radiological capsule containing cesium-137 from its protective housing in a teletherapy machine. One of the thieves punctured the 1-millimeter-thick window of the capsule, contaminating the surrounding areas as the capsule was transported and the radioactive material dispersed. As a result of contact with the radioactive material, four people died, and 249 people and 85 buildings were contaminated.

(U//FOUO) Terrorists have planned RDD attacks on at least one occasion:

- (U//FOUO) In November 2006, a London court sentenced Dhiren Barot to life in prison for planning terrorist attacks, including the planned use of an RDD in attacks in England. Barot conducted research into the possible health effects of the radioactivity released by burning thousands of smoke detectors that contained small amounts of radioactive americium-241.

(U) Key Components

(U//FOUO) To execute an RDD attack, terrorists must have the ability to obtain radioactive material and the means to disperse it so that the intended targets are exposed to radiation. Radioactive materials are used every day in food irradiation plants, for industrial use, in laboratories, and medical centers. If stolen or otherwise acquired, many of these materials could be used in an RDD. Varieties of radioactive materials—including cesium-137, cobalt-60, and strontium-90—could be used in an RDD.

(U) Methods of Attack

(U) The likelihood of localized effects leads many experts to agree that an RDD most likely would be used either to contaminate facilities or places where people live and work or cause anxiety in those who believe they are being or have been exposed. Terrorists likely would target an RDD at infrastructure with large concentrations of people to maximize the potential consequences of an attack. The cascading effects, however, could affect other sectors as well, since decontamination costs associated with an attack could be extensive.

(U) Radiological Dispersal Devices

(U//FOUO) Explosive RDDs or dirty bombs use the explosive force of detonation to disperse radioactive material. A simple explosive RDD consisting of a lead-shielded container, commonly called a "pig," with a kilogram of explosive attached could fit into a backpack.

(U//FOUO) Radioactive material could be dispersed in powder or aerosolized forms. For example, an airplane could disperse the material over an area, or terrorists could manually distribute radioactive material to target areas.

(U//FOUO) Atmospheric RDDs are intended to convert radioactive material into a form easily transported by air currents. Some amount of radiological material disseminated by an explosive RDD will be transported by air currents; however, only a device designed specifically for that purpose is considered an atmospheric RDD. For example, water-soluble radiological materials could be transported in pressurized sprayers used in home maintenance, landscaping, or pest control and sprayed at the potential target site.

(U) Radiological Exposure Devices

(U//FOUO) Terrorists could choose to place an RED in a densely populated area where people who come into contact with it are exposed to radiation. The degree of exposure would depend on factors such as the amount and type of radiological material. A strong RED could be placed in a densely populated or highly trafficked facility, which might expose a large number of people to intense radiation over a short time; a weaker RED

could be placed in an office space to harm a limited number of people over a long time. An RED attack most likely would be aimed at creating a psychological impact and economic effects because authorities probably would deny access to the affected area until the radioactive source was removed. This attack method would be unlikely to cause immediate casualties or destruction.

(U) Standoff Weapons: Guided

(U//FOUO) Terrorists could take advantage of the proliferation of guided missiles, such as man-portable air defense systems (MANPADSs) and man-portable anti-tank guided missiles (ATGMs). Terrorists have used standoff weapons overseas; however, some of these military systems may not be readily available in the United States. Standoff weapons pose a challenge to protecting facilities, since their ranges may provide terrorists the ability to negate most traditional perimeter defenses to damage, disrupt, or destroy CIKRs.

(U) Definition

(U//FOUO) A standoff weapon is any weapon that fires a projectile (or is a projectile itself) and is fired from beyond small arms range. Guided standoff weapons use a variety of methods to guide a missile to its intended target, including active, passive, and preset guidance. The intent and design of standoff weapons are to attack from a distance, and they are particularly useful when close access to a target is not feasible. Circumstances that would lead terrorists to use a standoff weapon include strong security or physical difficulty in reaching the target. This attack method focuses on two types of guided standoff weapons: MANPADSs and ATGMs.

(U//FOUO) **MANPADSs:** Commonly described as shoulder-fired anti-aircraft missiles, MANPADSs are short-range surface-to-air missiles that an individual or crew can carry and fire. Typical guidance systems or "seekers," include (1) infrared, which homes in on an aircraft's heat source, usually engine exhaust, (2) command line-of-sight, whereby the MANPADS operator visually acquires the target aircraft using a magnified optical sight and radio controls to guide the missile into the target, and (3) laser beam riders, in which the missile flies along a laser beam and strikes the aircraft where the operator has aimed the laser. Types of MANPADSs that could be used in this attack method include the Soviet or Russian manufactured SA-7, SA-14, and SA-18; the French-produced Mistral; and the U.S.-made FIM-43 Redeye, FIM-92 Stinger, Blowpipe, Starburst, and Starstreak.

(U//FOUO) MANPADSs generally have a target detection range of about 5.6 miles and an engagement range to 4 miles; therefore, aircraft flying at 20,000 feet or higher are relatively safe. MANPADSs (the firing tube with a missile inside), typically range from 4 to 6.5 feet long and are about 3 inches in diameter. Their weight with launcher ranges from 28 to more than 55 pounds. They are easy to transport and relatively easy to conceal. Depending on the model, MANPADSs can be purchased on the black market in

several countries for a few hundred dollars for older models to approximately $250,000 for newer, more capable models.

(U//FOUO) **ATGMs:** More than 50 types or versions of anti-tank guided missiles exist. These missiles are designed to destroy heavily armored vehicles and tanks. ATGMs are divided into two categories based on their primary delivery methods: mounted and dismounted. The U.S. tube-launched, optically tracked, wire-guided (TOW) system is one of the most widely available ATGMs ever fielded. The TOW, because of its size, is usually a mounted weapon. Dismounted ATGMs are a more likely threat to CIKRs, given their smaller size and cheaper cost. Some dismounted ATGMs include the Fire Arrow, Milan, and AT-3 Sagger (one of the versions is sometimes referred to as a "suitcase Sagger" because the missile can be fired from a portable suitcase launcher).

(U) Background

(U//FOUO) **MANPADSs:** Terrorists have targeted airliners using MANPADSs and other standoff weapons since the 1970s. Most terrorist MANPADSs attacks have been against aircraft, but MANPADSs could be used to target vulnerable ground facilities, particularly any asset that gives off a heat signature.

(U//FOUO) Approximately 20 countries have produced or have licenses to produce MANPADSs or their components. In addition to the United States, these include Bulgaria, China, Egypt, France, Germany, Greece, Iran, Japan, Korea, Montenegro, Netherlands, North Pakistan, Poland, Romania, Russia, Serbia, Sweden, Turkey, and the United Kingdom. An estimated 1 million MANPADS missiles have been manufactured worldwide to date. Most of these systems are in national inventories or have been destroyed, but many others exist for which no accounting has occurred.

(U//FOUO) Terrorists could use a variety of means to obtain guided missiles, including arms dealers, black markets, international organized crime, theft, and transfers from willing states. MANPADSs form part of the arsenal of weapons available to almost 30 insurgent and terrorist groups worldwide, and their proliferation on the black market may make them relatively easy to acquire.

— (U//FOUO) In 2005, British businessman Hemant Lakhani attempted to sell shoulder-launched missiles to what he thought was a terrorist cell that planned to shoot down aircraft in the United States.

— (U) In December 2002, International Security Assistance Force troops in Afghanistan reportedly were offered FIM–92A "Stinger" MANPADSs for $250,000 each. Conservative estimates put at least 100 such missiles as still unaccounted for, out of approximately 900 originally supplied to Afghan insurgents fighting the 1979–1989 Soviet occupation of Afghanistan.

(U//FOUO) **ATGMs:** ATGMs have capabilities and pose threats similar to those of MANPADSs. The military uses ATGMs in infantry formations against both light and heavy armor; virtually every military in the world has ATGMs. ATGMs are readily available on black markets overseas.

(U) Key Components

(U//FOUO) **MANPADs:** Most MANPADs consist of a missile packaged in a tube; a launching mechanism (commonly known as a "gripstock"); and a power supply. The tube is disposable and has an aiming device, which sometimes integrates with the gripstock. The tube also protects the missile until it has been fired. The missiles themselves contain the homing and guidance devices that direct them toward their target.

— (U//FOUO) Some experts assess that MANPADSs missiles have a finite shelf life, but a technically proficient terrorist group probably could replace perishable components such as electronic systems batteries with improvised or fabricated equivalents. The life of the missiles is enhanced because they are shipped in sealed containers designed to protect them when deployed in the field. Under ideal conditions, the lifespan of some MANPADS missiles is estimated to be more than 20 years.

(U//FOUO) **ATGMs:** Each system has different key components, but in general ATGMs consist of a launch platform and a missile with a guidance system. ATGMs primarily use explosive-shaped charges in their warheads because their primary purpose is to penetrate armor.

(U) Methods of Employment

(U//FOUO) Standoff weapons have been designed for specific military purposes. MANPADS are developed as close-in weapons for use against low-flying tactical aircraft and helicopters. Anti-tank weapons are designed for use against armored vehicles. Terrorists can and will adapt weapons for use against other targets, including critical infrastructure.

(U//FOUO) **Use of MANPADSs to attack aircraft in flight:** Terrorists could fire MANPADSs at aircraft in flight to cause the aircraft to break apart or crash. Aircraft in the early or terminal stages of flight are most vulnerable because they are traveling at relatively slow speed, at low altitude, and usually are moving in a straight line. An attack from the rear of the aircraft would be most effective because of the heat signature from the engines. In 2003, the U.S. Department of State estimated that since the 1970s more than 40 civilian aircraft have been hit by MANPADSs, causing approximately 25 crashes and more than 600 deaths.

— (U//FOUO) The most recent attempted shoot down of a civilian passenger aircraft was in November 2002 in Mombasa, Kenya. Two SA–7 missiles were

fired at, but missed, an Israeli-registered Boeing 757 aircraft operated by Arkia Israeli Airlines. The attack was believed to have been carried out by terrorists linked to al-Qa'ida.

— (U//FOUO) On 10 October 1998, a suspected SA–7 downed a Congo Airlines Boeing 727 near Kindu, Democratic Republic of Congo. The missile reportedly struck the airplane's rear engine, causing a crash that killed all 41 persons on board.

(U//FOUO) **Unconventional use of MANPADSs:** Terrorist groups are known to be innovative in their weapons employment and could attempt to use guided standoff weapons against infrastructure assets other than aircraft. For example, numerous infrastructure assets have heat signatures and may be vulnerable to MANPADSs attacks.
(U//FOUO) **Unconventional use of ATGMs:** The characteristics of ATGMs that make them effective tank killers (shaped charge, high-explosive warheads) also lend themselves to use against other targets, such as critical infrastructure assets. ATGMs potentially could penetrate critical structures that lack protection against a standoff attack.

(U) Standoff Weapons: Unguided

(U//FOUO) Standoff weapons are used by terrorists and insurgents overseas. Some of the standard military standoff systems used by terrorists may not be readily available in the United States; however, terrorists can fabricate weapons that have similar characteristics. Standoff weapons pose a challenge to facilities since their ranges may allow attackers to negate most traditional perimeter defenses to damage, disrupt, or destroy CIKRs.

(U) Definition

(U//FOUO) An unguided standoff weapon is any weapon that launches a projectile (or is a projectile itself) that follows a basic ballistic trajectory that does not alter in flight. Unguided standoff weapons fall into four general categories: artillery, mortars, small arms, and unguided shoulder-fired rockets. These categories follow general military-type definitions. Most countries manufacture unguided standoff weapons for their militaries, but terrorists also improvise standoff weapons with similar characteristics.

— (U) **Artillery:** Artillery normally is a medium-to-heavy, very large-bore (rifled or smoothbore) weapon that fires a fuzed projectile. Artillery weapons are either towed or self-propelled. The intent and design of artillery are for both barrage and specific target attacks from a distance of a few hundred yards to dozens of kilometers. Targets most often are out of the line of sight.

— (U) **Mortars:** A mortar is a light artillery weapon usually with ammunition loaded through the muzzle of the barrel (or "tube"). A mortar fires a fuzed projectile indirectly at the target through a high-arcing ballistic trajectory. The

weapon fires shells at low velocities and at short range relative to other artillery weapons. The effective range of mortars and mortar systems can be from 100 meters to more than 7,000 meters. Noted for having short barrel lengths relative to their projectiles, mortars fire shells that can accommodate a variety of mission-specific fuzes. Most mortars are light enough to hand-carry or transport in light vehicles to firing areas; they also can be fired from disguised or modified vehicles.

— (U) **Small arms:** Small arms, such as medium and heavy machine guns and long-range rifles, especially those that use ammunition 7.62 mm or larger, can be used for unguided standoff attacks. Extended and heavy barrels enable longer effective ranges for standard rifles, which usually have a range of approximately 400 meters. Specialty sniper and large-caliber rifles may have effective ranges to 1,500 meters.

— (U) **Unguided shoulder-fired rockets:** The intent and design of unguided shoulder-fired rockets are to counter entrenched personnel and armored vehicles at close range and to breach obstacles and penetrate fortified structures. Many countries produce such weapons. The rocket-propelled grenade (RPG) is the most common type of ammunition used and is commonly fired from a hand-held launcher based on the Russian PG–7. The PG–7 has many variants, and its portability and choice of warheads have made it a weapon of choice for guerrilla forces. The majority of weapons of this type are relatively light systems that a single person can carry and deploy, and they generally have a maximum effective range (powered flight) of 300 meters.

(U//FOUO) Terrorists can create improvised standoff weapons based on the materials, skills, and tools available to them. For example, since 2002 the Palestinian terrorist group HAMAS has used improvised Qassam rockets against Israel; these rockets are made of steel tubes filled with explosives. HAMAS terrorists reportedly hide a Qassam in a truck, drive to a clearing near the Gaza border, and launch the rocket. In addition, reporting indicates that the Irish Republican Army as of 2002 colluded with the Revolutionary Armed Forces of Colombia on the employment of improvised mortars.

(U) Background

(U) **Artillery:** Terrorist groups have used artillery in many attacks overseas against a variety of targets. For example, HAMAS and Hizballah have fired artillery randomly into Israel primarily to cause terror among the Israeli population.

(U) **Mortars:** Mortars are a preferred weapon of terrorists in Afghanistan and Iraq because they can be transported from a firing area immediately after use. Mortars are notable for the highly arced trajectory of their projectiles, which often provides enough time for terrorists to flee the firing area before the projectile reaches its target. Lightweight mortar systems tend to have a low profile and can be camouflaged or

concealed easily. Lightweight systems also often are designed for quick assembly and disassembly. Operatives in Iraq have used such systems to attack civilian targets such as outdoor markets and places of worship.

(U) **Unguided shoulder-fired rockets:** The RPG–7 and its variants are some of the most widely used RPGs in the world; the militaries of approximately 40 countries use the weapon, and it is manufactured in a number of variants by at least seven countries. The weapon has cheap but effective sights, and operators require only limited training to attain proficiency. The Afghan mujahidin used them extensively during the 1980s to destroy Soviet vehicles. They remain a preeminent weapon for insurgents in places such as Afghanistan, Chechnya, Iraq, and Sri Lanka.

(U) **Small arms:** Terrorists have used small arms in many attacks. Some small arms, especially large-caliber rifles and anti-material rifles, could be used in attacks against CIKRs to terrorize personnel or to puncture or harm critical assets.

(U) Key Components

(U) **Artillery:** In general, most modern artillery systems comprise several components, including the gun (barrel and breech), carriage, cradle, recoil system, and some way of transporting the system, such as integration with a vehicle or appendage to a wheeled base. Common field artillery ammunition comprises three major components: projectile, projectile fuze, and the propellant.

(U) **Mortars:** Most modern mortar systems comprise three main components: a tube (barrel), a base plate, and a bipod. Typically a projectile (shell) is dropped down the tube onto a firing pin causing ignition of the (shell-integrated) propellant to launch the round. Generally, heavy mortars, those 107 mm in diameter or larger, require trucks or tracked vehicles to move them, although they are still considerably smaller than artillery weapons.

(U) **Unguided shoulder-fired rockets:** These systems comprise two main parts: the launcher and the round. The most common types of warheads are high-explosive anti-tank (HEAT) rounds. These warheads are affixed to a rocket motor and stabilized in flight with fins. The launcher normally is a tube that focuses the rocket exhaust to create thrust, causing the warhead to be propelled at the target. Unguided shoulder-fired weapons usually are light enough to be carried and fired by one person. An RPG team usually comprises at least two people: the shooter and the person who carries additional rockets, reloads the weapon, and serves as a spotter and defender for the shooter. The launch of an RPG–7, no matter how well camouflaged, leaves a tell-tale blue-gray smoke signature that can reveal the launch location.

(U) **Small arms:** Small arms, whether long-range rifles or machine guns, consist of actions, barrels, and triggers. Most modern firearms are loaded with metal cartridges that contain a metallic projectile or bullet, a powder propellant, and a primer for ignition. A

bullet can be made simply of lead, or augmented with chemical illuminators or incendiaries, or specially designed to pierce armor. Most modern firearms are equipped with detachable magazines, which increase cartridge capacity, decrease the need to reload, and allow greater rates and volumes of fire. The type of small arm and the cartridge used will determine the effective range.

(U) Methods of Employment

(U//FOUO) How a terrorist will employ an unguided standoff weapon likely will vary depending, among other things, on the type of weapon and the skill of the attacker. This section outlines two possible terrorist methods of employment of the unguided standoff weapon:

(U//FOUO) **Attack against a target in motion:** Terrorists could use an unguided standoff weapon to attack targets such as armored vehicles, standard vehicles, vessels, or fixed- or rotary-wing aircraft. An RPG is relatively imprecise against a moving target at its maximum range of 900 meters; therefore, attackers likely would operate in proximity to the target. Firing RPGs at proximity has proven extremely effective against rotary-wing aircraft and slow-moving vehicle convoys, and could be employed along transportation routes. Large-caliber rifles and machine guns would be effective against targets in motion, since terrorists would be able to acquire targets with much more accuracy and precision, and the continuity of fire would enable closer tracking of the target.

(U//FOUO) **Attack against a stationary target:** This method of attack involves terrorists using artillery, mortars, or small arms against stationary targets such as buildings, compounds, or docked ships. The chances for success increase with multiple weapons or weapon types, but terrorists could attack with only one weapon. A stationary target affords terrorists more time to plan and develop an effective attack from greater distances. Terrorists could launch rockets from mobile systems, allowing them to vacate the immediate area before the shell lands or before security elements can respond. Alternatively, terrorists could use standoff weapons including small arms to terrorize people at a facility. An attack could include sniper tactics and random attacks to instill fear and cause loss of life and economic consequences.

(U) Vehicle-Borne Improvised Explosive Device

(U//FOUO) VBIEDs are an attractive attack option for terrorists since they provide a large, mobile device capable of causing significant damage and casualties. VBIEDs are one of the most likely terrorist devices to cause mass casualties.

(U) Definition

(U//FOUO) VBIEDs integrate a vehicle and an explosive device specifically for detonation against a target. The vehicle can be used to deliver large quantities of explosives to a target and can help disguise the intent of the attack. VBIEDs constitute large, mobile, difficult-to-detect weapons capable of causing significant behavioral impact, loss of life, and structural and economic damage. VBIEDs do not include the use of a vehicle to transport explosive material for placement outside the vehicle or an explosion within a vehicle not intended to inflict damage to an external target.

(U//FOUO) Nearly any type of vehicle can be used in VBIED attacks: buses, cargo vans, fuel tankers, motorbikes, passenger cars or limousines, pickup trucks, and tractor trailers. (IEDs delivered by means other than vehicles are addressed in a separate section. Boats rigged with explosives intended for detonation against a target are defined as "Maritime Vessels as Weapons" and also are addressed separately.)

(U) Background

(U//FOUO) Almost every major terrorist organization—including al-Qa'ida; the Basque Homeland and Freedom in Spain; the Irish Republican Army (IRA) in Northern Ireland and England; and the Revolutionary Armed Forces of Columbia—has executed VBIED attacks. Vehicles are readily available, and many types of explosive material are relatively easy to acquire. Large VBIED attacks have caused hundreds of casualties.

(U) Key Components

(U//FOUO) A VBIED is an IED that incorporates a vehicle in its design and employment. VBIEDs vary widely in shape and form, but they share a common set of components:

- (U//FOUO) **Vehicle:** A Department of Defense analysis of about 200 worldwide VBIED incidents revealed that in more than 77 percent of the attacks, the perpetrators used compact or standard size sedans. They used passenger or cargo-type vans in 4 percent of the incidents and box vans or trucks in 8 percent. In four incidents attackers used motorcycles or rickshaws to transport and conceal the explosive device. Other types of vehicles used in VBIED attacks included bicycles and trailers.

- (U//FOUO) **IED:** Along with the vehicle, most VBIED employs four basic elements common to all IEDs: power supply, initiator, explosives, and switch or sensor. Some IEDs use other mechanisms instead of an electric power source, such as the case with Oklahoma City Bombing. The effectiveness of the VBIED does not depend solely on the amount of explosive content. Each element of a device can be tailored specifically to suit the attack scenario. Components can be

crude or sophisticated, depending on the skill, resources, and requirements of the bombmaker and the attack environment.

(U//FOUO) When a VBIED detonation occurs, three effects cause destruction and injury: blast, fragmentation, and thermal.

— (U//FOUO) **Blast:** The blast is caused by overpressure resulting from a near-instantaneous conversion of solid or liquid explosives into rapidly expanding hot gases. The blast can knock down buildings and propel objects and people great distances.

— (U//FOUO) **Fragmentation:** Terrorists may choose to include materials that, upon detonation, will generate high velocity fragmentation. Alternatively, they may choose to detonate a VBIED close to materials anticipated to cause additional or collateral damage. Fragmentation typically is categorized as primary or secondary. Primary fragmentation consists of shattered pieces of the explosive device, sometimes referred to as "shrapnel." Fragmentation also can result from the deliberate inclusion of objects such as ball bearings, nails, or other hardware into the design of the IED. Such objects can be externally affixed or mixed with an explosive filler, and are sufficiently strong to survive the blast and to puncture skin when propelled by force. Secondary fragmentation is nearby debris propelled by the blast, but at a lower velocity than primary fragmentation.

— (U//FOUO) **Thermal:** The thermal effect contributes relatively little compared with the damage from the destructive force, since the fireball generally will not exceed the blast radius.

(U//FOUO) Terrorists could attempt to enhance the effects of an IED with additional materials, such as toxic industrial chemicals or chemical warfare agents.

— (U//FOUO) On at least three occasions in January and February 2007, insurgents in Iraq incorporated chlorine tanks in VBIED attacks. Most of the deaths from the attacks were caused by the explosion, but many people were treated and hospitalized for chlorine exposure.

(U) Methods of Employment

(U//FOUO) Terrorist groups have used various means to conduct VBIED attacks and will continue to seek innovative ways to employ them, including combinations of the types.

(U//FOUO) **Sanctioned or Disguised Vehicle:** This technique uses stolen delivery, emergency, or official vehicles, or vehicles that resemble them. An advantage of this tactic lies in the ability of the driver to approach and position the VBIED without arousing suspicion or to enter limited or controlled access areas unnoticed.

— (U//FOUO) On 29 January 2004, terrorists detonated a 500-pound bomb concealed in a disguised Red Crescent ambulance outside the Shaheen Hotel in Baghdad, killing four.

— (U//FOUO) In early 2004, Dhiren Barot devised extensive plans to blow up limousines packed with gas cylinders and explosives in parking lots under key buildings in the United States and the United Kingdom. He judged the limousines would appear official and therefore be less subject to scrutiny and that their large storage capacity would afford the terrorists maximum space for explosives, thus increasing the likelihood of a successful operation.

(U//FOUO) **Abandoned Vehicle:** This commonly used tactic involves terrorists positioning and then abandoning the vehicle prior to the explosion. After arriving at the target, they may abandon the vehicle after initiating a timer, or remain nearby to detonate the device remotely.

— (U//FOUO) In the April 1995 attack on the Murrah Federal Building in Oklahoma City, Timothy McVeigh parked a rental van filled with more than 4,000 pounds of homemade explosives in front of the building and abandoned it after lighting a fuse. The VBIED killed nearly 170 people and injured more than 650.

— (U//FOUO) In February 1993, al-Qa‘ida associate Ramzi Yousef led the team that abandoned a rental van packed with explosives in the underground parking garage of the World Trade Center. The attack killed six people and injured more than 1,000.

(U//FOUO) **Suicide VBIED:** This tactic involves a terrorist driving or riding in the vehicle to the target and detonating the explosives while occupying it. This tactic helps to inflict maximum damage and casualties by allowing the attacker to more precisely determine the optimum time and location to detonate the device. In addition, a vehicle usually can get past security personnel or obstacles allowing little or no time for security to react. Most of al-Qa‘ida’s VBIED attacks are suicide missions.

— (U//FOUO) On 7 August 1998, al-Qa‘ida operatives conducted nearly simultaneous suicide vehicle bombings at U.S. Embassies in Dar es Saalam, Tanzania and Nairobi, Kenya killing 224 people and wounding more than 5,000.

— (U//FOUO) JI, an Indonesian Islamic terrorist organization loosely affiliated with al-Qa‘ida, carried out suicide VBIED attacks against a hotel in Jakarta on 5 August 2003 that killed 12 people. Another JI-perpetrated VBIED attack on Australian Embassy Jakarta in September 2004 killed 9 people and injured 182.

(U//FOUO) **Proxy VBIED:** In some cases, terrorists force or deceive a proxy into driving an explosives-laden vehicle to a target where the terrorists then detonate the explosive. It is possible that the driver of or passengers in the vehicle are not aware the vehicle is a VBIED; alternatively, they may know it is a VBIED, but are not aware they are participating in the execution of an actual attack.

— (U//FOUO) On 24 October 1990, a group of IRA members kidnapped Patrick Gillespie from his home, held his family hostage, and told him to drive a van to a vehicle checkpoint on the Donegal border in Northern Ireland. IRA operatives followed Gillespie to the border checkpoint where they detonated the bomb in the van.

(U) **Reporting Notice:**

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to DHS and/or the FBI. The DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@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. The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. 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 the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) **Tracked by:** HSEC-010000-01-05, HSEC-030000-01-05, TERR-060000-01-05