Assessment

(U) Homeland Security Threat Assessment: Evaluating Threats 2008-2013

IA-0058-09

Office of Intelligence and Analysis
ASSESSMENT

(U) Homeland Security Threat Assessment: Evaluating Threats 2008–2013

(U//FOUO) Prepared under the auspices of the Strategic Analysis Group, Homeland Environment Threat Analysis Division, Office of Intelligence and Analysis. Inquiries may be directed to SAG at 202-282-8165 or 202-282-8690.

(U) This Assessment was approved by the Homeland Security Intelligence Council under the authority of the Under Secretary for Intelligence and Analysis, U.S. Department of Homeland Security.

(U) Information as of August 2008 was used in the preparation of this Homeland Security Threat Assessment.

(U) The following organizations participated in drafting this assessment: Department of Homeland Security/Office of Intelligence and Analysis; Homeland Environment Threat Analysis Division; Borders, WMD, and Health Threat Analysis Division; and Critical Infrastructure Threat Analysis Division.

(U) DHS coordinating organizations are Immigration and Customs Enforcement, U.S. Secret Service, U.S. Coast Guard, U.S. Customs and Border Protection, Transportation Security Administration, and U.S. Citizenship and Immigration Service.

Table of Contents

(U) Scope

(U//FOUO) The 2008 Homeland Security Threat Assessment (HSTA) is a strategic assessment looking out five years. The HSTA represents the analytical judgments of the Department of Homeland Security (DHS) Intelligence Enterprise (IE) regarding the critical threats to the U.S. Homeland that the Department will need to address in the period 2008-2013. These threats are organized into six major categories:

- (U//FOUO) Demographics and travel security;
- (U//FOUO) Border security;
- (U//FOUO) Chemical, biological, radiological, and nuclear security;
- (U//FOUO) Health security;
- (U//FOUO) Critical infrastructure; and
- (U//FOUO) Domestic extremism and radicalization

(U//FOUO) The estimates in this assessment are designed to prevent surprise by explicitly highlighting threats that could result in an incident of national significance. Each of the categories of strategic threats is assessed in the following contextual framework:

- (U//FOUO) Enduring threats that DHS/IE believes will persist and continue to challenge the Homeland security community through 2013.

- (U//FOUO) High consequence, uncertain probability threats that could result from a dramatic departure from current trends, resulting in threats of greater significance.

(U) Methodological Note

(U//FOUO) Representatives from across DHS/IE postulated more than 100 candidate enduring threats and high consequence, uncertain probability threats. Those selected for this assessment represent DHS/IE's collective judgment of the most relevant threats that could significantly affect Homeland security.

(U//FOUO) In addressing threats for which DHS has principal or significant responsibility, this assessment does not cover natural disasters because other government agencies, such as the National Weather Service and National Oceanographic and Atmospheric Administration, have well-established roles providing information on such events. The exception is global diseases that could affect U.S. citizens or food production. The major threat categories do not cover the full scope of statutory responsibilities of the individual DHS components; for example, the safety of navigation responsibilities of the U.S. Coast Guard.

(U//FOUO) DHS uses a five-point scale to define the potential consequences of a threat (see Appendix). This scale considers three factors: loss of life, economic damage, and psychological impact. For this assessment, the focus is on the mid-to-high end of the scale—threats that could have moderate, significant, catastrophic, or severe consequences.

(U//FOUO) The HSTA provides key inputs for Departmental planning and programming activities, such as the Quadrennial Homeland Security Review. It has been coordinated within the Department and approved by the Homeland Security Intelligence Council, which is chaired by the Under Secretary for Intelligence.

(U) Executive Summary

(U//FOUO) The 2008 Homeland Security Threat Assessment (HSTA) focuses on a broad array of threats for which the Department, its Components, and its State, local, and tribal partners must prepare, protect, prevent, and respond. First among these is the crosscutting threat of a terrorist attack originating from either external or internal actors. The Department of Homeland Security (DHS) Intelligence Enterprise (IE) has identified six distinct categories of threats—demographics and travel security; border security; chemical, biological, radiological, and nuclear (CBRN) security; health security; critical infrastructure; and domestic extremism and radicalization. These threats may emanate from abroad, impact our borders, or rise within the United States. DHS/IE categorizes them as enduring threats and assesses that they will affect Homeland security through 2013, or as high consequence threats that could have a dramatic effect given a change in intent or capability of threat actors.

(U) Enduring Threats

(U//FOUO) ***Demographics and Travel Security:*** Demographic pressures abroad and illicit travel introduce new and potentially growing challenges to securing the Nation's borders and ports of entry. At the highest level of concern, terrorists will attempt to defeat border security measures with the goal of inserting operatives and establishing support networks in the United States to conduct attacks. Islamist extremists, militia members, drug dealers, criminals, and other illicit transnational actors will attempt to evade travel security measures through document fraud, obtaining illicit documents, or attempting to exploit legal U.S. admission programs such as the Visa Waiver Program (VWP). These illicit actors also could pose as refugees or asylum seekers to gain access to the United States. State failure and internal conflicts abroad will continue to generate sizable refugee flows to the United States—notably from countries of special interest for terrorism in the Middle East, Africa, and South Asia—which could provide opportunities for illicit entry into the United States.

(U//FOUO) ***Border Security:*** Mexican drug-trafficking organizations will continue to undermine security along the U.S. southern border. The potential for extremists or terrorists to cross the northern border from Canada is a serious potential risk. A variety of cross-border crimes occur to differing degrees along both the U.S. southern and northern borders, such as alien smuggling, money laundering, and trafficking in arms and other contraband. Often interrelated, many of these criminal activities support or facilitate each other and shape the overall threat environment along the borders.

(U//FOUO) Transnational criminal organizations are adapting to border security measures by using new routes and technologies. Of particular note are the use of semi-submersibles and the expanded use of tunnels along the southern border.

(U//FOUO) ***Chemical, Biological, Radiological, and Nuclear Security:*** The most dangerous functional capabilities that U.S. adversaries aspire to use to attack U.S. citizens and key elements of U.S. political, economic, or social life are CBRN weapons.

Al-Qa'ida and its affiliates will remain intent on acquiring and using CBRN weapons. Their capabilities to conduct CBRN attacks, however, probably will remain low, with acquisition of materials continuing as their most significant challenge.

(U//FOUO) ***Health Security:*** Many threats to public health, both engineered and naturally occurring, have the ability to cause catastrophic damage to the Homeland. A variety of naturally occurring diseases could significantly affect the health of U.S. citizens, undermine Homeland food supply, and threaten the economic stability of the U.S. agricultural industry. Avian influenza is one potentially serious infectious disease threat to U.S. public health and agriculture. Even a small-scale, intentional food contamination hoax or incident could have widespread consequences to include deaths, hospitalization, loss of consumer confidence, and national and international economic impacts.

(U//FOUO) ***Critical Infrastructure:*** Threats to Homeland critical infrastructure and key resources, whether from transnational or domestic actors, primarily come from two principal methods—physical attacks and the increasingly worrisome potential of cyber attacks. Al-Qa'ida remains focused on Homeland targets that maximize economic loss, inflict casualties, and create political turmoil.

(U//FOUO) Nation-states are the most capable actors, but al-Qa'ida and other terrorist groups will continue to remain intent on developing or acquiring cyber attack capabilities. They currently lack those capabilities. The threat of cyber terrorism likely will increase over the next five years because of the proliferation and exploitation of advanced hacking tools. Youthful, Internet-savvy extremists might apply their online acumen to conduct cyber attacks rather than offer themselves up as operatives to conduct physical attacks.

(U//FOUO) ***Domestic Extremism and Radicalization:*** Small cells of violent Islamic and non-Islamic domestic extremists may attempt to conduct attacks inside the United States during the period of this assessment. U.S. persons who travel overseas for training are of particular concern. These attempts could resemble the plotting by the Fort Dix terrorists. These groups likely will lack the capability to conduct large-scale attacks without direct support from a transnational terrorist organization, but will be capable of conducting small-scale attacks. The pool of radicalized Islamists inside the United States likely will evolve during the next five years as extremists increasingly exploit the Internet to inspire a wave of young, self-identified Muslim "terrorist wannabes" who aspire to carry out violent acts. Non-Islamic domestic extremists have the means to conduct attacks, but their illicit activities likely will continue to be confined to smaller scale crimes—including hate crimes—and vandalism. Domestic non-Islamic extremists also are becoming more sophisticated in cyber capabilities and operational security procedures.

(U) High Consequence, Uncertain Probability Threats

(U//FOUO) In addition to the enduring threats identified above, high consequence threats of uncertain probability could emerge as significant dangers to the Homeland if a redline were crossed or a significant change in the intent or capability of threat actors

were to occur. The High Consequences portion of the HSTA is designed to identify events representative of the type and scale of activities contingency planners and policymakers may need to consider. ***The high consequence assessments that follow are not inclusive of all possible events; rather, they represent a selected set distilled from a larger set of candidates which could significantly impact Homeland security.***

(U//FOUO) These developments could occur if an enduring threat were to intensify rapidly or depart dramatically from DHS/IE's current understanding of the threat, resulting in a much more significant threat. These departures would be driven by discontinuous changes in intent or capability. These estimates are designed to prevent surprise by explicitly highlighting threats that could result in an incident of national significance.

(U//FOUO) ***Demographics and Travel Security:*** DHS/IE identified two high consequence threats in this category that could emerge due to a change in threat actor intentions or an increase in foreign instability:

— (U//FOUO) Should Hizballah's intent to attack the Homeland change as the result of a significant triggering event, the group could attempt to infiltrate operatives from abroad to initiate attacks against symbolic or military targets.

— (U//FOUO) If terrorists were to gain access to a state-produced nuclear weapon, the obstacles to deploying it would be high. Terrorists would face a fundamental tradeoff between maintaining physical possession of a stolen or recovered weapon and risk of detection or loss of control inherent to transferring the weapon to intermediaries.

(U//FOUO) ***Border Security:*** DHS/IE identified a high consequence threat in this category that could emerge if U.S. borders were challenged by the consequences of a failed state:

— (U//FOUO) An uncontrolled mass migration could threaten the Homeland's ability to maintain security along U.S. borders. A failed Cuban leadership transition could shift the locus of Cuban illegal cross-border activity from the U.S. Southwest land border to southeastern maritime points of entry and challenge the Homeland's ability to maintain border controls.

(U//FOUO) ***CBRN and Health Security:*** A high consequence, uncertain probability threat could emerge if any one of a variety of "bad actors" obtains the capability to conduct a CBRN attack or if a highly virulent form of the H5N1 virus emerges that is highly pathogenic in humans.

— (U//FOUO) Any group would have to overcome the obstacles to manufacturing a biological weapon. If they were to succeed in obtaining a biological weapon—most likely anthrax or plague—they may well attempt an attack on a large urban area, which could have grave consequences.

— (U//FOUO) Similarly, the emergence of a highly virulent form of the H5N1 virus that is highly pathogenic in humans would result in an avian flu pandemic that rapidly would reach global proportions. The consequences to the United States could be severe because of the nearly universal lack of immunity of U.S. citizens.

(U//FOUO) ***Critical Infrastructure:*** Acquiring cyber attack capabilities could lead a variety of actors, ranging from nation-states to transnational criminals to terrorists, to launch cyber attacks targeting the U.S. economy or critical infrastructure.

— (U//FOUO) Computer network exploitation or computer network attacks could disrupt U.S.-networked critical infrastructure systems and "just-in-time" inventory and product distribution systems, crippling key sectors of the national economy.

— (U//FOUO) Criminal enterprises or terrorist groups could acquire the requisite cyber attack capabilities by outsourcing, corruption, or compromise and operate in an environment where it would be extremely difficult to detect the threat.

(U//FOUO) ***Extremism and Radicalization:*** Rightwing extremists' responses to government policies perceived threatening to their goals could escalate from an enduring threat to a high consequence, uncertain probability threat such as a large-scale bombing or smaller scale, coordinated bombings. Small domestic cells and lone wolves could execute copycat attacks whose sinister nature could extend adverse social or psychological effects nationwide.

(U) Introduction

(U) This is the second edition of the Homeland Security Threat Assessment (HSTA). It builds upon the foundation of the assessment last year and identifies significant changes as well as continuity regarding the dangers facing the Homeland. This assessment focuses on threats based on both intent and capability, for it is the combination of these two factors that most sharply characterizes the significance of these threats to the security of the Homeland.

(U) To maximize its utility to DHS leaders, Department Components, and partners in Federal, State, and local law enforcement, emergency response, and officials responsible for the security of critical infrastructure, the assessment covers the following strategic threats: demographic and travel security threats; threats to the border; chemical, biological, radiological, and nuclear threats; health security threats; threats to critical infrastructure; and threats posed by homegrown extremism and radicalization.

(U) Since the Department's areas of responsibility overlap with those of other Federal, State, and local government institutions, the HSTA identifies and reflects the assessments made by sister agencies and departments but focuses principally on those threats that are distinctly the concern of DHS. In this year's edition, DHS/IE has increased the focus on threats that affect State, local, and private sector partners to both highlight these threats and identify for DHS potential areas of increased interaction with those partners.

(U//FOUO) The major departure of the HSTA 2008 from its predecessor is that the 2008 version does not separately address international terrorism. The subject is addressed, where appropriate, within the six major threat categories. As a service to the reader, this Introduction concludes with a text box summarizing the Intelligence Community's (IC's) current understanding of the international terrorism threat to the Homeland.

(U) International Terrorism Overview

(U//FOUO) As the 2007 National Intelligence Estimate on "The Terrorist Threat to the U.S. Homeland" and the 2008 Interagency Intelligence Committee on Terrorism assessment on "The Worldwide Terrorism Threat" conclude, al-Qa'ida poses the greatest terrorist threat to the Homeland. DHS/IE concurs with that assessment. Al-Qa'ida will continue to influence and direct operations through its affiliated regional networks and through autonomous groups and networks inspired by al-Qa'ida and the global jihad. These autonomous groups commonly are referred to as homegrown or domestic extremists and will be discussed in further detail in the Extremism and Radicalization section of the HSTA.

(U//FOUO) Al-Qa'ida has steadily rebuilt elements of a Homeland attack capability in the establishment and maintenance of a safehaven in Pakistan's Federally Administered Tribal Areas (FATA), the assignment of operational lieutenants, the reestablishment of control by top leadership, and the continued recruitment and training of operatives capable of gaining entry to the United States.

(U//FOUO) Lebanese Hizballah may pose a terrorist threat to the Homeland over the next five years if it develops a specific Homeland intent. The IC assesses, however, that absent a perceived existential threat to Hizballah, its leadership, or Iran, Hizballah will simply remain a capable, well-resourced terrorist organization without specific intent of conducting attacks against the Homeland. The IC also assesses that U.S.-based Hizballah is engaged in local fundraising through "charity" projects and criminal activities to include money laundering, smuggling, drug trafficking, fraud, and extortion.

(U//FOUO) The threat from international terrorism will continue to affect the Homeland in a variety of ways over the period of this assessment. Terrorists continue to be an adaptable adversary. The IC assesses that terrorists continuously consider exploiting a variety of licit and illicit tactics to access the Homeland, including the use of regional affiliates with the potential to exploit immigrant and nonimmigrant programs such as the Visa Waiver Program (VWP). The specifics of these threats from the perspective of Homeland Security intelligence will be examined in further detail in the main body of this assessment.

(U//FOUO) Enduring Threats

(U//FOUO) Enduring threats are strategic threats that DHS/IE believes will endure throughout the period of this assessment and that will continue to challenge the Homeland security community.

(U) Demographic and Travel Security Threats

(U//FOUO) Refugee Flows

(U//FOUO) State failure and internal conflict will continue to generate refugee flows to the United States, notably from countries of special interest for terrorism in the Middle East, Africa, and South Asia. Unfavorable economic and political conditions

in these regions, large expatriate populations in the United States, long waits for legal U.S. immigration, and increasingly restrictive European refugee and asylee admissions programs likely will result in increased use of illicit means to gain entry to the United States.

(U//FOUO) According to the UN High Commissioner for Refugees, more than 4.5 million Iraqis are currently displaced—2.4 million inside Iraq and close to 2.2 million outside the country. The United States plans to admit 12,000 Iraqis through the U.S. Refugee Admissions Program during Fiscal Year 2008.[1]

— (U//FOUO) Between 1 October 2006 and 6 August 2008, DHS/United States Citizenship and Immigration Services (USCIS) interviewed more than 24,300 Iraqi refugees, approving refugee status for just over 16,600 of them. Of those, approximately 10,600 have arrived in the United States. In 141 cases—approximately 0.6 percent of the total individuals interviewed—derogatory information led DHS/USCIS to deny the applicant refugee status.

(U//FOUO) The number of Iraqis attempting to migrate to the United States—through both licit and illicit means—probably will increase over the next five years as a result of harsh refugee policies in neighboring countries such as Jordan and Syria and increasingly restrictive European refugee and asylee programs. Ease of access to human smuggling and fraudulent document networks likely would underpin such an increase.

— (U//FOUO) DHS/Customs and Border Protection (CBP) apprehended 392 Iraqis illegally attempting to cross U.S. borders and at ports of entry (POEs) in FY 2007; 224 Iraqis, or 57 percent, attempted to enter at the San Ysidro, California POE.[2,3,4]

— (U//FOUO) Iraqis attempting to reach the United States have been detained and found to possess fraudulent—often photo-substituted or impostor—Bulgarian, Cypriot, Dutch, German, Greek, Italian, Polish, Romanian, and Swedish passports, often obtained from European-based human smugglers. Many Iraqis travel through Turkey and Greece to Western Europe, where they board flights to Mexico or another Latin American country for onward movement to the United States.[5,6,7,8,9]

(U//FOUO) Refugee flows in Africa, particularly in Somalia and Sudan, could increase as a result of renewed conflict there. Lower U.S. refugee admissions ceilings for Africa—a proposed 16,000 in FY 2008, down 27 percent from 22,000 in FY 2007—could lead to increased illicit immigration to the United States.[10] Refugees attempting illegal migration would have access to well-established smuggling operations.

(U//FOUO) Events over the next five years in Afghanistan, Bangladesh, and Pakistan—countries experiencing instability due to a variety of internal factors—could lead to increased immigrant flows to the United States, providing extremists or other illicit actors new opportunities to mask their movements from South Asia. A surge in demand for U.S. refugee resettlement from Pakistan, in particular, could burden U.S. travel and

refugee programs. In FY 2007, individuals with Pakistani citizenship represented the third-largest number of positive Terrorist Identities Datamart Environment (TIDE) match encounters, following individuals with U.S. and Canadian citizenship.[11]

(U//FOUO) Licit and Illicit Travel

(U//FOUO) Consistent with the 2007 HSTA, DHS/IE assesses that illicit actors, including terrorists, will seek access to the United States through both licit and illicit means. They will use a variety of tactics to enter the United States, to include recruiting U.S. citizens who can enter and exit the country freely, exploiting nonimmigrant and immigrant programs, and traveling to the United States using travel documentation from VWP countries.

(U//FOUO) Extremists, including al-Qa'ida-affiliated groups active in regions affected by failed-state and conflict-driven migration, could attempt to use fraudulent and fraudulently-obtained documents to gain access to U.S. travel programs.

(U//FOUO) Based on past practice, al-Qa'ida probably retains a preference for legal entry into the United States, thus maximizing freedom of movement once inside the country.

— (U//FOUO) The disrupted UK-based aviation plot in August 2006 involved British citizens who had trained in Pakistan. The UK-based plotters would have been eligible to board a U.S.-bound plane using legitimate UK passports.

(U//FOUO) Al-Qa'ida's regional affiliate structure also may enhance access to recruits with Western travel documentation for facilitated access to the United States, such as through the VWP. Over the past year, al-Qa'ida announced mergers with the former Algerian Salafist Group for Preaching and Combat (now known as al-Qa'ida in the Land of the Islamic Maghreb) and the Libyan Islamic Fighting Group.[12,13] Both of these groups have well-established support networks in Europe and North Africa. The Islamic Jihad Union (IJU) also maintains an extensive network worldwide that al-Qa'ida could access. Individuals involved in the thwarted September 2007 IJU plot in Germany received terrorist training in Pakistan.

(U) Threats to the Borders

(U) Drug Traffickers and Extremists

(U//FOUO) The greatest immediate challenge to U.S. borders remains the ability of Mexican drug trafficking organizations to smuggle large amounts of illicit drugs into the United States, amass immense profits, and exert greater influence over Mexican law enforcement, local political officials, and other criminal groups operating along the border. Despite the early successes from the comprehensive counterdrug strategy launched by President Felipe Calderon, drug cartels are determined to hold their

monopoly on smuggling routes to the United States.[14,15] Continued successes by Mexican and U.S. counterdrug efforts are placing significant pressures on the cartels and may further disrupt the rough equilibrium that existed between them. The resulting increased violence and shifting alliances may affect the entire criminal landscape along the border and the related threats posed to the Homeland by alien smuggling, arms trafficking, and, potentially, the entry of terrorists and terrorist weapons into the United States.

— (U//FOUO) As much as 90 percent of the cocaine and the majority of marijuana and methamphetamines enter the United States from Mexico, as does most of the heroin consumed west of the Mississippi River.[16,17]

— (U//FOUO) Two major cartels dominate the trafficking of drugs into the United States. The Gulf Cartel/Los Zetas, based in Tamaulipas, controls most smuggling routes along the eastern side of the U.S. Southwest border. The Sinaloa Cartel, based in western Mexico, is engaged in violent competition with the Gulf Cartel for control of smuggling corridors. The once powerful Arellano-Felix Organization, based in Tijuana, has lost influence because of the arrests of key leaders.[18]

(U//FOUO) Recently launched counternarcotics efforts by the U.S. and Mexican Governments have had some successes in curtailing the influence of criminal organizations along the U.S. Southwest border, yet these organizations remain resilient.

— (U//FOUO) Since taking office in December 2006, Calderon has undertaken a series of aggressive and unprecedented actions against the drug cartels, including military-led counterdrug operations, sweeping anticorruption campaigns targeted at judicial and law enforcement entities, and regional security initiatives with the United States and Central American countries. These actions have led to arrests of several significant cartel figures, large quantities of seized drugs, and extradition of drug traffickers to the United States.[19,20]

— (U//FOUO) Violence on both sides of the U.S. Southwest border continues to increase. Drug-related murders in Mexico—most of which occur in the border region—have risen sharply in 2008, reaching almost 3,000 by the end of August and on track to reach 4,500 by year-end.[21] A combination of interrelated factors is driving drug cartel violence along the border, stemming from increased clashes with Mexican military and police, inter- and intra-cartel conflict, and efforts to intimidate Mexican counterdrug officers as the cartels continue to compete for control of lucrative smuggling corridors to the United States.

(U//FOUO) Crossing the border from Mexico illegally along the U.S. Southwest corridor has become more challenging because of an array of new U.S. security enhancements, such as those implemented under the Secure Border Initiative. These efforts have increased significantly the number of border agents, aerial surveillance assets, and physical barriers along the border to detect and disrupt cross-border criminal activities.

— (U//FOUO) Increased border security and law enforcement on the U.S. side of the border have placed further pressures on Mexican drug and alien smugglers, who are increasingly directing violence against U.S. border personnel. Violence against DHS/CBP personnel increased by 28 percent to more than 1,000 in FY 2007 and numbered 326 during the first quarter of FY 2008, a 43 percent increase over the same period in FY 2007.[22,23] Border violence will continue to increase, if the United States and Mexico are able to sustain pressure and disrupt the Mexican drug cartels.

(U//FOUO) The absence of large Islamic or ethnic communities in Mexico limits the ability of terrorist operatives to blend in or gain support for crossing the border. Moreover, Mexican drug and alien smuggling organizations have little incentive to risk their lucrative operations by facilitating terrorists across the border. Al-Qa'ida planners view infiltration of the U.S. Southwest border to be one potential option for entering the United States.[24]

— (U//FOUO) Approximately 5,000 Muslims are believed to reside in Mexico among a total population of 107 million. Mexican Muslims are dispersed widely throughout the country and, unlike a number of other North American Muslim populations, are not a cohesive community.[25]

(U//FOUO) Canada could offer an attractive option for potential terrorists to attempt entry to the United States because of its proximity and the high volume of cross-border traffic in which to blend. Most of Canada's 32.6 million inhabitants—more than 6 million of whom are foreign-born (2006 census)—live within 100 miles of the border. The amount of trade and tourism across the U.S.-Canada border is vast—greater than that between the United States and the entire European Union.

(U//FOUO) A number of known extremist groups operate in North America seeking to exploit a significant demographic pool potentially susceptible to radicalization. Members or affiliates of foreign terrorist organizations—including al-Qa'ida, HAMAS, Hizballah, several north African groups, Liberation Tigers of Tamil Eelam, and Babbar Khalsa International—have been identified among Muslim, Tamil, and Sikh communities in Canada.[26]

(U//FOUO) Sympathy with foreign terrorist organizations' goals has allowed at least one Canadian independent homegrown group to plot attacks. The so-called "Toronto 18" group of Canadian extremists planning attacks against multiple Canadian targets in June 2006 had U.S. and international connections, but received no leadership or direction from any identified foreign terrorist group.[27,28]

(U//FOUO) U.S. Northern border land POE watchlist encounter patterns suggest extremist interest to enter the United States from Canada. No terrorist operatives, however, have been encountered among watch list hits at U.S. Northern border land POEs since 1999. DHS/CBP Border Patrol apprehensions of watch listed individuals between the POE stations along the U.S. Northern border are extremely rare.

— (U//FOUO) DHS/IE assesses that terrorists would be unlikely to use fraudulent travel documents at U.S. Northern border land POE stations or cross between the POEs unless unable to obtain legitimate documents.

(U//FOUO) Drug smuggling from Canada into the United States represents a smaller percentage compared with drug smuggling across the U.S. Southwest border, but is a significant concern because some types of trafficking have increased recently and likely will continue to increase through the period of this assessment. Canada is the primary source country for MDMA (ecstasy) entering the United States and is a significant and growing producer of high-potency marijuana.

(U//FOUO) Highly flexible smuggling organizations are likely to adapt and change their operational tactics in response to new and increased border security capabilities along both borders.

— (U//FOUO) The continuing proliferation of cross-border tunnels in recent years—a record 19 new tunnels were discovered on the U.S. Southwest border in 2007—suggests that Mexican drug traffickers are reacting to increased U.S. and Mexican counterdrug operations.[29]

(U) Smuggling and Money Laundering

(U//FOUO) The use of small conveyances bypassing border enforcement measures is increasing. The increased presence of border security measures at the U.S. Southwest and maritime borders has forced smugglers to step up their exploitation of perceived detection vulnerabilities through the use of small aircraft, boats, and submersibles.

(U//FOUO) Inland waterways at the U.S. Southwest and Northern borders offer smuggling organizations opportunities to evade detection in areas where law enforcement resources are limited.

(U//FOUO) Drug trafficking organizations are using innovative methods to bring illicit goods into the United States, as illustrated by the rising use of submersibles. Unlike submarines, submersibles operate with visible pilot houses and exhaust tubes above the waterline, while the hull remains submerged to decrease the vessel's overall profile.

— (U//FOUO) U.S. and Colombian patrol boats in 2007 seized 13 submersible vessels, more than the total number of craft seized during the previous 14 years combined.[30]

— (U//FOUO) The Mexican Navy in July 2008 for the first time interdicted a submersible carrying a cocaine shipment.[31,32]

(U) Submersible smuggling craft.

(U//FOUO) Prepaid debit and cash cards provide criminals with opportunities to transfer illicit funds in and out of the United States without being detected.
Resembling credit cards, prepaid debit cards could enable criminals to bypass border security measures.

— (U//FOUO) Funds are prepaid and withdrawn through ATMs anywhere in the world. Drug smuggling organizations use these cards as their primary means to transfer funds across the border.[33]

— (U//FOUO) Colombian smuggling organizations have used prepaid cash and debit cards to launder and transfer funds by depositing money in one country and withdrawing it in another.[34]

(U) Chemical, Biological, Radiological, and Nuclear Threats

(U//FOUO) DHS/IE's assessment of al-Qa'ida's CBRN aspirations remains consistent with those of the 2007 HSTA. Al-Qa'ida leadership historically has given high priority to chemical, biological, radiological, and nuclear attacks to achieve mass casualty goals, and DHS/IE judges that their interest will endure through the period of this assessment. DHS/IE assesses that al-Qa'ida and like-minded groups will continue their pursuit to develop, acquire, and use CBRN weapons against the Homeland. DHS/IE judges that al-Qa'ida's and other terrorist organization's capabilities to conduct such attacks could include release of toxic chemicals, explosive dissemination of radiological material (a radiological dispersal device) or aerosol dissemination of pathogens.

(U//FOUO) Domestic Terrorist Groups Show Little Interest in a Sophisticated CBRN Capability

(U//FOUO) DHS/IE assesses that no domestic extremist groups are systematically working to develop or improve a CBRN attack capability. Domestic extremists historically have used commercially or industrially available toxic industrial chemicals, and simple dissemination techniques. Their plots generally are limited in scope, aimed at a specific target, and not focused on producing mass casualties. DHS/IE assesses that lone actors are more likely to perpetrate a CBRN attack, but there are few cases from which to draw conclusions. The vast majority of attempted and successful domestic terrorist CBRN attacks have used chemical weapons. DHS/IE judges that toxic industrial chemicals and toxins probably will remain the attack method of choice for domestic actors seeking to use CBRN because of their availability and the relative ease of making them into weapons. DHS judges that this pattern of domestic extremist CBRN use will continue over the next five years.

— (U//FOUO) Only three cases involving domestic extremist attempts to either produce or procure chemical weapons have been confirmed since 2001.

— (U//FOUO) Between 1993 and 2007, at least 16 confirmed ricin incidents involving domestic extremists have occurred; none resulted in any fatalities.

— (U//FOUO) Individuals in the United States have attempted to acquire radiological materials—such as by harvesting material from smoke detectors—for the purpose of constructing a radiological dispersal device.[35] This methodology, however, would not result in an effective radiological dispersal device because of the minimal amount of radioactive material used in smoke detectors.

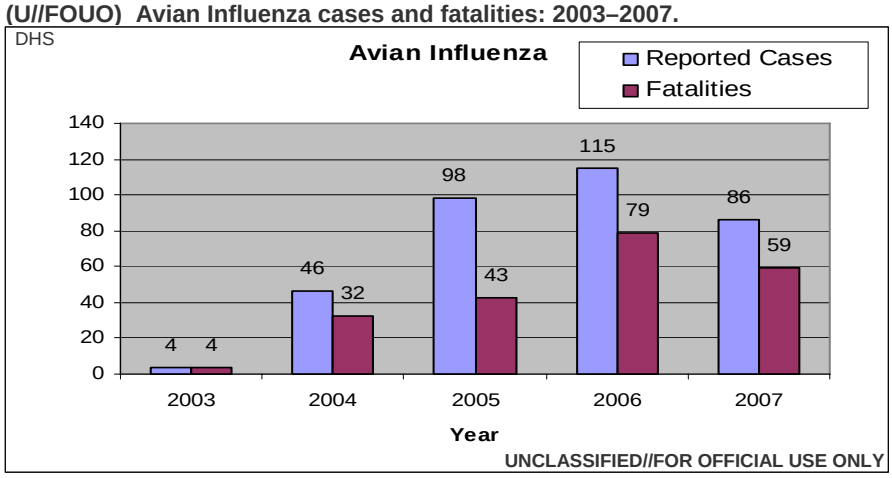
(U) Health Security Threats

(U//FOUO) Infectious Human and Agricultural Diseases

(U//FOUO) DHS/Office of Intelligence and Analysis (I&A) judges that a pandemic of any highly transmissible and virulent disease has the potential to severely strain the Homeland's medical and public health infrastructure. Highly pathogenic avian influenza (HPAI) strain H5N1 is a potentially serious threat to animals and humans in the United States. In addition, the emergence of a novel, highly transmissible and virulent human respiratory illness for which the United States has no countermeasures, such as the SARS coronavirus, could pose a significant new threat.

(U//FOUO) In 2007, approximately 23 percent fewer confirmed human HPAI (H5N1) cases and 25 percent fewer fatalities were reported by the World Health Organization (WHO) than in 2006, whereas the official case fatality rate remained unchanged at 69 percent.[36] DHS/IE cannot attribute the decline in cases and fatalities to one specific cause but judges that increased biosurveillance, a relatively milder climate, public education, and aggressive culling in response to outbreaks in poultry may have contributed to the reduced incidence of human H5N1.

(U//FOUO) Avian Influenza cases and fatalities: 2003–2007.



(U//FOUO) At present, no strain capable of causing sustained human-to-human transmission has emerged from currently circulating H5N1 strains. Small clusters of suspected limited human-to-human transmission of H5N1, however, have been observed.[37,38] DHS/I&A assesses that H5N1 will continue to cause sporadic cases of human illness and death in the developing world in limited numbers. Mutations that may allow for a greater adaptation in mammals have been identified in H5N1 strains isolated from both infected birds and human cases, although these strains still are unable to efficiently transmit from human to human.[39] DHS/IE cannot predict the likelihood that a novel (non-H5N1) pandemic strain will emerge, although new influenza stains could emerge from mutation or reassortment of currently circulating influenza strains.

(U//FOUO) Global health security against infectious disease is a significant challenge because of weak detection capabilities and inconsistent international reporting on diseases around the world. A variety of factors may contribute to the delay in identifying a disease outbreak. Most important is the ability and willingness of developing nations to diagnose and rapidly report on disease outbreaks, including emerging infectious diseases. Reporting delays may be exacerbated by underlying political or economic motives, both locally and nationally, to disguise or minimize the social and economic impacts of a disease outbreak.

(U//FOUO) The U.S. agriculture industry is vulnerable to deliberate or accidental contamination. The potential for a foreign animal disease or plant pathogen to be introduced into the Homeland by human activity—inadvertently, deliberately, or by natural phenomena—poses a significant threat. Mechanisms for inadvertent introduction include imports or smuggling of infected animals or animal products, plants, food, or other goods.

(U//FOUO) An outbreak of H5N1 in the United States would have severe economic consequences for the domestic poultry industry. In 2007, H5N1 circulated widely in domestic poultry and wild birds in many countries in Africa, Asia, and Europe. These outbreaks resulted in the culling and destruction of millions of birds in more than two dozen countries.

- (U) A 2002 outbreak of low pathogenicity avian influenza (LPAI) (H7N2) in Virginia and West Virginia resulted in the destruction of 4.7 million birds and an estimated economic loss of $130 million.[40]

- (U) A smaller LPAI (H5N2) outbreak occurred in West Virginia in 2007.[41]

(U) As of January 2008, H5N1 has not been detected in the Western Hemisphere. Other HPAI influenza strains, however, including subtypes H5N2 and H7N3, have in previous years caused outbreaks in poultry in the United States, Canada, Chile, and Mexico.[42] DHS/IE judges that bird smuggling and introduction by migratory birds are two likely routes for H5N1 to enter the Western Hemisphere.

(U) Low Pathogenicity and High Pathogenicity Avian Influenza

(U) Media reporting on avian influenza outbreaks often fails to explain the distinction between high pathogenicity (HPAI) and low pathogenicity (LPAI) avian influenza strains. LPAI infections, which normally cause only mild or undetectable illness and few fatalities, occur frequently in wild birds, which subsequently can infect poultry. HPAI strains usually cause severe illness and high mortality in wild birds and poultry, but some bird species, including ducks, can be asymptomatic carriers of some HPAI strains, including H5N1. Some viral isolates also may be designated as HPAI based on laboratory testing.

(U) For some subtypes, including H5N1 and H7N3, both low pathogenicity and high pathogenicity strains have been observed. Mutation of LPAI strains into HPAI strains has been observed in poultry flocks. Humans can become infected with both HPAI and LPAI strains, although thus far, only HPAI strains have caused human fatalities. To date, LPAI infections have caused only mild symptoms in humans.

(U//FOUO) Contamination of the U.S. food supply is a continuing threat. Food products are vulnerable to contamination at many points, especially during production, storage, and transport. Imported food potentially is more vulnerable because monitoring processes at various stages may be less rigorous. A successful attack on the U.S. food system could have severe economic and health effects.

— (U//FOUO) Previous incidents demonstrate that even small groups can mount contamination attacks that can harm large numbers of people and cause widespread economic and social effects.

— (U//FOUO) The March 2007 discovery that foreign manufacturers were adulterating wheat flour, wheat gluten, and rice protein concentrate used as ingredients in animal feed and pet food with melamine prompted extensive disruptions in domestic commerce, product recalls, and at least short-term loss of consumer confidence.

(U) Threats to Critical Infrastructure

(U) Explosive Threats

(U//FOUO) Consistent with the 2007 HSTA, DHS/IE assesses that al-Qa'ida remains focused on Homeland targets that maximize economic damage and loss of life and create political turmoil. The U.S. transportation and energy sectors, along with iconic targets, remain the most likely al-Qa'ida targets during the period of this assessment. Al-Qa'ida's most significant challenge to achieving these goals remains the ability of its trained operatives to gain entry into the United States to conduct attacks.

(U//FOUO) Terrorist groups have demonstrated the ability to conduct attacks using improvised explosive devices (IEDs), and this method is the most common form of attack. IEDs can be made from common, off-the-shelf consumer products that are easy to acquire. Using homemade explosive devices (HMEs) reduces or eliminates the need to risk purchase or theft of regulated commercial or military explosives, presenting

authorities with fewer opportunities to detect and disrupt terrorist plots. Instructions for making IEDs are taught in terrorist training camps, published in terrorist manuals, and widely available on the Internet.

— (U//FOUO) The 2005 Madrid bombers used devices containing stolen, commercially manufactured dynamite as a main charge.

— (U//FOUO) The September 2007 bombing plot in Germany, the August 2006 airline plot originating in the United Kingdom, and the July 2005 London transit attacks all involved use of HMEs based on hydrogen peroxide. The 1995 Oklahoma City bombing used a mixture of ammonium nitrate and nitro-methane racing fuel.[43]

— (U//FOUO) In December 2001, Richard Reid attempted to use triacetone triperoxide (TATP) to initiate the less sensitive, homemade pentaerythritol tetranitrate (PETN) in the shoe bomb he wore aboard an airliner destined for Miami.

(U//FOUO) The ready availability of these materials worldwide and the relatively simple steps for production of HMEs make these materials particularly challenging to detect and provide terrorists with an opportunity to employ simple technologies to conduct bombing operations.

(U//FOUO) Terrorists have demonstrated clearly both the intent and capability to employ IEDs. Hizballah is the group most capable of conducting a bombing campaign, but has not demonstrated any intent against the Homeland. Insurgency campaigns, such as those in Afghanistan, Chechnya, India, Iraq, Lebanon, Pakistan, and Sri Lanka, have used IEDs with success. Terrorists have refined the design, manufacturing, and deployment of IEDs in the Afghanistan and Iraq theaters, significantly increasing their effectiveness.

(U//FOUO) Speculating on a Change in al-Qa'ida Explosives Strategy

(U//FOUO) DHS/IE believes al-Qa'ida will continue to pursue a goal of spectacular explosives attacks on critical infrastructure and iconic Homeland targets using highly trained, security-savvy operatives. That said, if al-Qa'ida were to expand its attack options to include a campaign of multiple and frequent attacks on softer targets, the implications for Homeland security would be significant.

(U//FOUO) Hardened targets, strategic setbacks, and an abundance of volunteers could drive the paradigm shift. A plausible convergence of forces could drive al-Qa'ida to pursue a campaign using smaller attacks on soft targets. Such plots would develop over shorter time frames and involve less complex tactics, reducing the chances for failure.

— (U//FOUO) A possible key objective of such a strategy would be to strain local authorities by widening the potential set of softer targets that require protection. The 2002 D.C. sniper case and the accompanying media-driven fear illustrate the potential effects of this type of campaign.

(U//FOUO) Such a shift could achieve psychological and social strains that have effects well beyond the physical impact or immediate casualties inflicted. In addition, the attacks could exacerbate latent fissures in U.S. society. For example, an attack on a Shia mosque or an Orthodox Jewish neighborhood could ignite ethnic or sectarian strife in the United States that, from al-Qa'ida's perspective, would be a desired outcome that advances its political goals.

— (U//FOUO) The Internet provides an easy access venue for the proliferation of knowledge about advances in IED technology, HME production, and employment techniques.

(U) Homegrown extremists generally limit their violence to less complex attacks on property or individuals and have used IEDs in the past to further their objectives.

(U) Cyber Threats: Nation-States, Terrorists, Criminals

(U//FOUO) Cyber attacks hold the potential for the disruption of computer network systems throughout the United States, including Federal, State, local, and tribal governments and the private sector. Because of the distinct role DHS plays in protecting the Nation's public and private cyber infrastructure, this year's edition introduces a cyber-security section addressing related issues in greater depth.

(U//FOUO) Motivated by economic, political, military, and ideological rationales, a wider range of threat actors are increasing their capabilities to conduct cyber attacks against the United States. ***Islamic terrorists remain intent but generally lack the capability to conduct cyber attacks against the United States. Nation-states have the greatest capability to engage in cyber attacks.*** Criminal organizations are engaging in cyber activities for financial gain and target governments, private industries, and individuals. In addition, criminal organizations and independent hackers offer a wide array of hacking tools and services to those willing and able to purchase them, which could provide terrorists with the attack capabilities they currently lack.

(U) Computer Network Operations (CNO) is an umbrella term that encompasses the various subdivisions in computer networking activity.

— (U) **Computer Network Exploitation (CNE)** is that set of activities associated with gathering information about a target computer or network to include scanning for vulnerable access points compromising those vulnerabilities and using the compromised resources to maintain access, stage computer code for later use, or for data exfiltration.

— (U) **Computer Network Defense (CND)** is the set of activities designed to protect system resources from exploitation or attack to include monitoring for, filtering, and blocking damaging and unauthorized activities.

— (U) **Computer Network Attack (CNA)** describes an offensive activity conducted by computer to modify, disrupt, deny, degrade, or destroy computers and networks or the information stored in computers. A computer network attack can affect the integrity and availability of data. CNA can be used to manipulate equipment controlled by computing systems.

(U) Nations as Cyber Threat Actors

(U//FOUO) Foreign nations are the most capable and resource-rich cyber threat actors. The most advanced nations have established active and robust information operations (IO) or CNO organizations. Some nations' military and intelligence agencies

have created distinct directorates to carry out aspects of IO, such as CNE, CND, and CNA. Several nations conduct cyber espionage against political, economic, and military targets in the United States.

— (U//FOUO) Only a handful of nations have all of these capabilities; the IO capabilities of other, less capable nations will continue to mature over the next five years.

(U) Cyber Terrorist Threats

(U//FOUO) Al-Qa'ida and other terrorist groups will continue to mature their cyber attack capabilities over the medium-to-long term, enabled by the proliferation of increasingly sophisticated cyber hacking tools. Al-Qa'ida and other terrorist groups will continue to remain intent on developing or acquiring cyber attack capabilities but currently lack those capabilities. Al-Qa'ida openly has stated its intent to attack critical infrastructure and key resources in the United States. Yet, most terrorist groups have not exhibited advanced cyber capabilities, other than limited denial of service attacks and website defacement. Large-scale attacks, such as disrupting metropolitan utility service, require a greater capability than DHS/IE assesses terrorist groups have.

(U//FOUO) Al-Qa'ida may well consider purchasing advanced hacker tools or hiring hackers to conduct attacks. The proliferation of hacking tools and related technology offer terrorist groups the opportunity to acquire the tools needed to carry out smaller attacks. Criminal organizations and independent hackers have developed a wide array of hacking tools and services that they offer to anyone willing and able to purchase them. Such tools could provide terrorists with capabilities they lack to conduct cyber attacks.

(U//FOUO) Al-Qa'ida and other Islamic extremist groups remain intent on maturing and employing cyber attack capabilities.

(U) Cyber Criminals

(U//FOUO) Cyber criminals, who have demonstrated significant capabilities by exploiting advanced cyber tools, are the greatest non-state threat to the U.S. economy, to include critical infrastructure and key resources (CIKR). Criminal organizations have a history of exploiting cyber systems for financial gain and will target governments, private enterprises, and individuals.

(U) Criminals use cyber attacks primarily for economic gain, seeking to steal financial information and extort money from public and private entities. Financial institutions and other businesses and their customers are targeted, with losses in the United States reportedly exceeding $20 billion annually.[44] The number of fraudulent or suspicious online financial transactions rose dramatically in 2007, largely because of computer hacking and malicious software attacks.[45]

(U) Cyber extortion is a growing threat to the United States, as criminals threaten to destroy valuable hardware or data and deny access to system resources.[46] Cyber extortion scams demanding payment in return for protection against network intrusions and distributed denial-of-service attacks are becoming more common and more sophisticated, according to press reporting.

(U) Cyber criminals appear disinclined, for now, to attempt national or regional level attacks in the United States because of challenges presented from the variety of architectural network infrastructures. Conducting a large-scale attack would require considerable time and resources to gain and maintain access to these networks. Smaller scale, targeted attacks focused on valuable key components or critical nodes of CIKR, however, could affect a service provider and create cascading effects. Actors targeting entities for extortion might prove elusive to law enforcement because of the lack of consistent reporting by infrastructure owner-operators and the difficulties of attribution in cyber space. Targeted entities might prefer to pay cyber criminals rather that disclose their vulnerability, risk loss of consumer confidence, or risk increased—and unwanted—governmental regulation.

— (U//FOUO) In February 2008, a Russian hacker informed a U.S. business that he had hacked its servers, allowing him to decrypt customer credit card numbers and other sensitive information. The hacker sought to extort $30,000 from the business in exchange for not publishing the company's security vulnerabilities. If the payment was not received, the hacker threatened to inform the firm's customers of the hack and that it was unsafe to use the company's services.[47]

(U//FOUO) New Digital Generation of Terrorists and Criminals

(U//FOUO) An increasingly technologically savvy generation, inspired by both Islamic and non-Islamic extremist ideologies, is emerging and filling more prominent roles in extremist movements. These next-generation extremists, including young women, could complement and support extremist goals by applying their online acumen rather than offering themselves up as operatives for kinetic attacks. A segment of the next generation also may represent a movement away from group oriented radicalization in favor of individual action in support of extremist ideologies.

(U//FOUO) Online recruitment and propaganda are broadening outreach to Western recruits. The increasing potency and ubiquity of digital and online media outlets give terrorists and other extremists added leverage to exploit what they believe is a vulnerable pool of recruits.

(U//FOUO) The number of social networking sites likely will grow and be exploited by extremists to communicate and recruit. An increasing number of young individuals establish and maintain social connections through these sites, providing cover to extremists seeking to mask their communications and activities. According to open source reporting, some criminal gangs target and groom middle-school children for membership using social networking sites.[48]

(U//FOUO) Online venues could, to some extent, supplant group-centric radicalization. Younger audiences using online forums could selectively find individuals or groups that support ideals that validate their unique extremist goals and perspectives. Forum groups could generate a new environment where new extremists feel empowered to act outside the guidance and control of a centralized organization.[49] Individuals from this young cohort already have emerged through online venues to align themselves with terrorist and extremist groups to which they are sympathetic.[50] Such an environment, for example, might well convince some of the newer extremists that the online instruction they receive is an acceptable alternative to the pedagogy of the militant mosque and therefore a potentially powerful incubator for the lone wolf extremist.

(U) Threats Posed by Homegrown Extremism and Radicalization

(U//FOUO) This section of the HSTA focuses on threats resulting from domestic extremists and associated radicalization activities. DHS/IE concentrates on two of the broadest and most threatening movements: (1) Islamic-based radicalization that supports violent change and (2) domestic extremism centered on racial or religious hatred, violent antigovernment views, or single-issue extremist groups such as abortion or animal-rights militants.

(U//FOUO) Islamic Extremists: Self-Generated Small Cells

(U//FOUO) The primary concern for the Homeland from the perspective of a domestic terrorist threat continues to be the potential generation of a few small, self-recruited or homegrown cells inspired by extremist-derived ideologies that justify and advocate the use of violence.

(U//FOUO) The spread of extremist propaganda on the Internet by Islamic terrorist organizations provides the rationale, inspiration, and even virtual training for a wave of young, impressionable radicals who self-identify as Muslims and aspire to carry out violent acts. The recent increase in volume of these radical messages, combined with sophisticated targeting of specific audiences in the United States, likely will expand the pool of susceptible recruits.[51]

(U//FOUO) Extremists arrested in North America were involved with Salafi networks that preach a literalist doctrine that may have cultivated an atmosphere of acceptance of the al-Qa‘ida worldview. These networks exist in a few newly established Islamic charitable and educational institutions in large urban centers that are run by young, charismatic religious leaders with links to extremist groups. This persistent and potent mix of factors may, over the period of this assessment, inspire a small number of self-initiated cells to conduct small-scale attacks. These groups, however, likely will lack the capabilities requisite to conduct spectacular, large-scale attacks without facilitation support from al-Qa‘ida.

(U//FOUO) Absence of Small-Scale Violence

(U//FOUO) Producing significant numbers of casualties or psychological effects is not difficult, as evidenced by the Washington, D.C. sniper case or the school shootings that have occurred in the United States and other countries. It is unclear why so few domestic extremists have exploited this inherent vulnerability, although an aspirational example suggests at least one attempt to do so:

— (U) Federal authorities in December 2006 arrested Derrick Shareef[USPER] after he attempted to purchase grenades and weapons for attacking a shopping mall food court in Rockford, Illinois to further his goal of "violent jihad."

(U//FOUO) Self-recruited Sunni extremists are inspired by a radicalized Salafi-Jihadist worldview, epitomized by al-Qa'ida's focus on targeting the United States and its allies. Their radical message focuses protest against what they claim is an anti-Muslim-oriented U.S. foreign policy or in support of "defensive jihad" overseas. Their vitriolic rhetoric, however, rarely translates into committing violence. Recent reported cases of cells or individuals aspiring to violence displayed a lack of training and sophistication. The al-Qa'ida tactical message, however—including indiscriminate, mass casualty attacks in the Homeland—resonates with self-recruited extremists and provides them future justification for transforming rhetoric into violent action. Currently, violent radicalization is less pronounced in the United States compared with other Western countries, although factors—such as the increasing role of Internet propaganda—could widen the scope and degree of activity over the forecast period.

(U//FOUO) Radicalization among some American Muslims is occurring via independent, decentralized networks that bring together extremists and susceptible youth attracted by virtual, ideological, and institutional factors. Increasingly, the Internet is transforming Islamic radicalization into a bottom-up phenomenon without linkages to state, regional, or national identity or group affiliation.

(U//FOUO) Some Islamic extremists have created Islamic educational institutions in North America that attract radicalized youth. Muslims across the Nation have been targeted by radical professors and influenced by radical leaders from student organizations.

(U//FOUO) Potential Cooperation among Islamic Extremists and Human Smuggling Networks

(U//FOUO) Human smuggling networks operate well-established transit routes into the United States that terrorists seeking illicit entry could exploit. To avoid the use of human-smuggling intermediaries and heighten operational security, extremists may establish criminal smuggling organizations more directly under their control.

(U) Sources:
(U//FOUO) NYPD Intelligence Division, *Radicalization in the West: The Homegrown Threat*, August 2007.
(U) The United States Attorney's Office Central District of California, *Two Plead Guilty to Domestic Terrorism Charges of Conspiring to Attack Military Facilities, Jewish Targets*, 14 December 2007.
(U) Southern Poverty Law Center Intelligence Report 2002.
(U) Phil Williams, "Early Warning Analysis: The Radicalization of Criminals and their Involvement in Terrorism," 2006.

(U//FOUO) Domestic Extremists: Capable of Violence on a Limited Scale

(U//FOUO) The major enduring threat from domestic extremist groups stems primarily from their capability to conduct small-scale attacks. Domestic extremist groups regularly cross the line from vociferous criticism to acts of harassing or even attacking their targets, although their actions usually are of limited scale and fall well within the purview of law enforcement. Several groups, however—particularly those espousing racist or violent antigovernment views—maintain substantial caches of arms and explosives that, if employed, would have significant physical or psychological impacts on the Homeland.

(U//FOUO) Animal-rights and environmental extremists are the most active domestic extremist groups, but white supremacists and militias are more violent and thus more likely to conduct mass-casualty attacks on the scale of the 1995 Oklahoma City bombing. Law enforcement and IC monitoring are therefore crucial for identifying tip-offs and indicators on any given group that may ramp up their tactics from aggressive rhetoric to large-scale violence.

(U//FOUO) Domestic Extremists Span the Ideological Spectrum

(U//FOUO) Domestic extremists organize around a full range of political, economic, religious, ethnic, or environmental issues and share a vehement conviction in the rightness of their views, which often are at odds with the population at large.

- (U//FOUO) On the extreme right, groups such as militia movements, neo-Nazis, and racist skinheads hold violent antigovernment and racist beliefs.
- (U//FOUO) Single issue extremists focus their energies on one cause. On the far left are groups that include animal-rights and environmental extremists; on the far right are groups that include antiabortion and anti-immigration extremists.
- (U//FOUO) Leftwing extremists, like violent revolutionary anarchists, are antigovernment but combine anticapitalist, antiglobalization, communist, and anarchist philosophies.

(U//FOUO) Decentralized networks offer increased operational security. Law enforcement sources report that extremist groups from across the political spectrum have evolved decentralizing tactics to bolster their operational security, deniability, and survivability.[52,53] Extremists appear to have adopted these tactics largely in reaction to successful law enforcement efforts to include infiltration operations as well as civil lawsuits filed against several well-known extremist groups.

- (U//FOUO) For example, countermeasures have galvanized rightwing extremists such as the National Socialist Movement[USPER] to direct their members to separate from the group when engaging in operational planning and preparations.[54] Consequently, factions or individuals that splinter from the parent group often hold the most radical views and propensity for violence and present the greatest challenge to identify and disrupt.

— (U//FOUO) Similarly, leftwing extremists, such as violent anarchists, animal-rights, and environmental groups, promote leaderless resistance tactics including operating in small, autonomous cells or individually to elude detection and complicate law enforcement operations.[55]

(U//FOUO) ***Rightwing extremists: Violent rhetoric, poor operational security.*** White supremacists—specifically skinheads—engage in the most extreme and virulent forms of speech and other public communications.[56] The IC, law enforcement, and open source reporting have identified activities that indicate intent by rightwing extremists to commit violent attacks using explosives or biological or chemical agents that could result in mass casualties.[57,58,59] These groups have limited operational capability to carry out such attacks, however, and plots of this nature have been disrupted. Reporting indicates that these groups are focused primarily on crimes against law enforcement officials and property as well as against members of ethnic or religious minority groups.[60]

(U//FOUO) White supremacists and militias possess the greatest capability of launching attacks on the scale of the 1995 Oklahoma City bombing. The more capable groups maintain large weapons caches and attract members with paramilitary skills—and, in some cases, individuals with formal military training.[61] White supremacist and militia Internet sites also offer instruction on how to prepare and conduct several kinds of attacks, including bombings, arsons, and poisonings. These groups, however, are challenged in the actual execution of complex plots and also are hindered by internal leadership struggles, immature tradecraft, poor operational security, law enforcement infiltration, and insufficient resources.

(U//FOUO) Animal-rights and environmental extremists are the most active of domestic groups.[62] Frustrated by their perceived lack of progress using peaceful means and spurred by the increasingly violent rhetoric of prominent movement figures, animal-rights and environmental extremists are becoming more active and confrontational. Groups such as the Animal Liberation Front and Earth Liberation Front welcome media attention on their harassment campaigns and attacks on targets they claim are linked to animal mistreatment and environmental degradation, believing this furthers their extremist causes.[63,64]

(U//FOUO) Animal-rights and environmental extremists have well-developed capabilities in surveillance, arson, and the use of small explosives and rudimentary capabilities employing industrial chemicals. They also are skilled in exploiting the Internet to disseminate tactics and techniques. In the coming years, they likely will further mature and refine their tradecraft, emboldening them to increase arson attacks and possibly use larger explosives.

(U) The Earth Liberation Front claimed responsibility for setting fire to four luxury homes in Woodinville, Washington on 3 March 2008.

(U//FOUO) Despite these groups' increasingly violent rhetoric, law enforcement reporting has not identified indicators signaling intent to carry out attacks designed to cause loss of life. Instead, these groups most likely will continue to use tactics such as setting fires, destroying property, and assaulting and harassing individuals and corporate interests they claim harm animals or degrade the environment. Their targets likely will continue to include the fur industry, testing laboratories using animals, construction sites they claim are environmentally offensive, and employees associated with these facilities and industries.

(U//FOUO) Certain government actions could further incite animal-rights and environmental extremists. Legislation or new regulations that they claim diminish animal protection or degrade environmental protection as well as the incarceration of fellow extremists could trigger these groups to rally supporters and spur violent acts.

(U//FOUO) Leftwing extremist activity is more sporadic and less lethal. Only small pockets of leftwing extremists, primarily violent anarchists, espouse the use of violence to advance their anticapitalist, communist, or socialist philosophies. They target government-owned buildings, military recruiting offices, and high-profile business and public events such as political campaigns, conventions, elections, and world trade and economic meetings. Their tactics include property destruction, vandalism, arson and fire bombings, sabotage, and violent protests. In the immediate near-term, their activities likely will remain at current levels through the U.S. Presidential transition period and as the war in Iraq continues, but will probably remain within the scope of local law enforcement.

(U//FOUO) Prisons will continue to be magnets for extremist recruiters. In these inherently violent and insular communities, extremist groups capitalize on inmates seeking protection from or status among other prisoners. Inmates are targeted for recruitment through outreach programs that include prison ministries and promises of security and stability upon their release from prison.[65] Once released, radicalized criminals frequently perpetrate crimes on behalf of the group, including the manufacture and selling of drugs and firearms to finance extremist operations.[66]

(U//FOUO) Islamic and Other Domestic Extremists: Internet Boosting Attack Capabilities and Recruitment

(U//FOUO) The attack capabilities of Islamic and other domestic extremists likely will mature in sophistication largely because of the proliferation of training manuals and videos available to them on the Internet. This interactive environment eases the efficiency and speed of communications to disseminate propaganda and provides an online repository for training manuals and how-to guides that can supplant access to information previously only available by field training. In addition, their awareness of successful law enforcement operations has spurred them to use tighter operational security practices and disseminate best practices to hinder intelligence gathering and investigations.

— (U//FOUO) An Internet-based extremist global network discovered in 2005–2006 included two college students from Atlanta indicted in 2006 on charges of conspiracy and material support who were directly linked to members of a homegrown cell of 18 individuals arrested in June 2006 in Toronto, which had acquired explosive materials, and to two Europeans arrested in Bosnia in late 2005 with plastic explosives.[67,68]

— (U//FOUO) The FBI and New York Police Department uncovered the Mohajroon Bulletin Board, a password-protected website hosted on a server in Houston that was a popular research site for Sunni extremists. Launched in early 2005, the site distributed to members detailed information on topics relating to paramilitary training for explosives, jihadist preparation, recruitment, and operational security. The site featured 18 forums that trained members on audio engineering and video production and editing along with polemics against non-jihadist or anti-jihadist groups. By April 2006, the bulletin board had 8,422 members before it was shut down one year later.[69]

— (U//FOUO) In 2007, a paroled militia leader in Michigan posted a series of paramilitary training videos to a popular media sharing website. Topics presented in these video lessons include field medical training, fire and maneuver exercises, field craft, and operating crew-served weapons. Propaganda pieces included aspirations to attack the United Nations and the Federal Government and to lynch judges and other government officials.[70]

— (U//FOUO) The Animal Liberation Front and Earth Liberation Front have posted multiple arson manuals on various websites. Handbooks such as “Arson Around with Auntie ALF,” “Final Nail 2,” and “Setting Fires with Electric Timers: An Earth Liberation Front Guide” provide step-by-step instructions and detailed diagrams, including how to prepare improvised incendiary devices.[71,72]

(U//FOUO) Abroad, al-Qa‘ida continues to significantly increase the quantity, quality, and sophistication of jihadist extremist propaganda targeting U.S. Muslims.

— (U//FOUO) Al-Qa‘ida-affiliated groups have expanded their efforts to reach a larger audience. In addition, the groups have improved the quality of their propaganda videos, graphics, and websites. Targeting audiences in specific demographic categories in English illustrates a more sophisticated marketing effort, most notably to American audiences to include African Americans, Latinos, and Native Americans.[73,74]

(U//FOUO) Domestic Extremists: Improving Operational Security, Propaganda, and Recruitment

(U//FOUO) Domestic extremists are adopting more rigorous operational security protocols. Successful law enforcement countermeasures, such as infiltration operations, have spurred domestic extremists to enhance security measures. White supremacist

groups, in particular, are more thoroughly vetting potential members, including requiring them to attend events where trusted members can evaluate and determine their commitment to the organization.[75] Maturing such countermeasures will continue to hinder State and local law enforcement efforts to monitor and investigate domestic extremist groups.

(U//FOUO) Domestic extremists increasingly will exploit advancements in information technologies to improve their propaganda and recruitment efforts. Enhanced networking and communication tools enable groups to promote extremist ideology, link with other extremist groups, and reach out to a wider audience with little fear of law enforcement interference. White supremacist groups use Internet sites to post paramilitary training videos and use a variety of members-only, peer-to-peer technologies that enable them to conduct organizational activities with enhanced operational control.[76]

(U//FOUO) High Consequence Threats of Uncertain Probability

(U//FOUO) Beyond the enduring threats assessed above, DHS/IE believes a number of high consequence threats could emerge over the time frame of this assessment that have low or uncertain probability of occurrence but that would have significant implications for the security of the Homeland. These threats warrant serious consideration by contingency planners and policymakers.

(U//FOUO) DHS/IE defines high consequence threats of uncertain probability as events that could result if one or more of the enduring threats previously identified were to develop in a much more threatening way. These developments could occur if an enduring threat were to intensify rapidly or depart dramatically from DHS/IE's current understanding of the threat, resulting in a much more significant threat. These departures would be driven by changes in intent or capability. These estimates are designed to prevent surprise by explicitly highlighting threats that could result in an incident of national significance.

(U) Demographic and Travel Security Threats

(U//FOUO) Insertion of Hizballah Operatives

(U//FOUO) A Hizballah campaign against the Homeland remains unlikely absent some significant triggering action. If triggered, however, Hizballah could infiltrate operatives from abroad to conduct mass-casualty attacks on government, military, Israeli diplomatic and commercial, and Jewish American targets.

(U//FOUO) The death of Hizballah terrorism chief Imad Mughniyah earlier this year could provide a motive to respond, but DHS/IE does not believe his killing alone will trigger Hizballah to attack the Homeland.

(U//FOUO) Movement of Uncontrolled Nuclear Weapons

(U//FOUO) If terrorists gained access to a state-produced nuclear weapon, the obstacles to deploying it would be high. Terrorists would face a fundamental tradeoff between maintaining physical possession of a stolen or recovered weapon and risk of detection or loss of control inherent to transferring the weapon to intermediaries. If a terrorist group were to succeed in detonating a state-produced weapon, the yield could be significant and produce casualties ranging from the thousands to the hundreds of thousands, depending upon proximity to a population center.

(U) Threats to the Borders

(U//FOUO) Southeastern Maritime Border Challenges

(U//FOUO) A failed Cuban leadership transition could result in a shift in illegal cross-border activity from the U.S. Southwest land border to southeastern maritime POEs.

— (U//FOUO) A weak or failing Castro or successor regime could provide even greater impetus for Cubans to flee the island. Such migrations—involving tens or hundreds of thousands of migrants—could occur by sea to Florida or indirectly by land through Mexico, overwhelming Homeland security resources to protect the U.S. southern border. Migrants and criminal organizations could seek to penetrate southeastern U.S. maritime points of entry.

(U//FOUO) DHS/IE assesses that since the Cuban National Assembly selected Raul Castro as Cuba's president on 24 February 2008, his tenure in the near-term will continue to instill a sense of stability and likely deter wholesale societal unrest.[77] ***Consequently, mass migration from Cuba is unlikely in the immediate future. Cuba's stability appears to be fragile, however, relying heavily on external financial support. Should this arrangement fail, the potential for a Cuban mass migration will become a high-consequence threat to the Homeland.***

(U//FOUO) A shift in illegal Cuban migration to the U.S. Southwest land border could be an indicator of a failed Cuban leadership transition. A migration pattern shift has occurred, characterized by an increasing influx of Cuban migrants illegally crossing the Mexican border into the United States. Cuban migrants and alien smuggling organizations (ASOs) are relying less on well-established southeastern maritime routes in favor of the U.S. Southwest land border. Cuban ASOs are using boats and other vehicles to transport illegal migrants from Cuba to Mexico to the U.S. Southwest border.[78] ***This shift, however, appears unrelated to the transition of Cuban leadership and more likely is a response by smuggling organizations attempting to evade increased U.S. border enforcement measures.***

(U//FOUO) DHS/IE assesses that, whereas the immediate political transition in Cuba appears to be stable, the fragility of the country's economy poses the potential for economic collapse that could spur illegal migration to the United States. Cuban citizens remain concerned about the future of their economic well-being.[79] The Government's inability to pay large international debts, coupled with public frustration over insufficient wages, could lead to economic instability and popular unrest.[80]

(U//FOUO) Indicators of Impending U.S. Southeastern Maritime Border Challenges

- (U//FOUO) An ineffective Cuban leadership transition results in reduced effective border control.
- (U//FOUO) Transnational criminal organizations use Cuba as a hub for illicit activities.
- (U//FOUO) Alien- and drug-smuggling organizations increasingly shift their routes from Mexico to Cuba.
- (U//FOUO) Cuban drug and alien smuggling activities rise.
- (U//FOUO) Cuban criminal networks increase their activities around U.S. Southeastern maritime points of entry.

(U//FOUO) In the past year, none of these indicators has been observed in response to the Cuban leadership transition.

(U) Chemical, Biological, Radiological, and Nuclear Threats

(U//FOUO) A Biological Attack on a Major Urban Center

(U//FOUO) DHS/IE judges that, over the period of this assessment, some terrorists will maintain an interest in developing the capability to conduct a biological attack. A spectrum of agents could be used in such an attack, but those of greatest concern combine a relative ease of production, environmental stability, and an ability to be disseminated in both wet and dry powder form.

(U//FOUO) A biological attack could affect a major urban center and, in the worst case scenario, infect up to hundreds of thousands of people. Such an event would temporarily overwhelm local health care systems with infected and worried citizens and might result in significant economic impact from worker illness or death.

(U//FOUO) Key components of an ability to conduct attacks using biological agents include the following:

- (U//FOUO) The possession of a viable pathogenic bacteria or virus. 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//FOUO) Indicators of a Biological Attack Plot

- (U//FOUO) The presence of terrorist operatives near outbreaks of threat diseases.
- (U//FOUO) Extremist infiltration of biosafety laboratories.
- (U//FOUO) Experimentation on animals.
- (U//FOUO) Purchase or interest in potential dissemination devices such as agricultural sprayers or foggers.
- (U//FOUO) Unusual outbreaks of disease.

(U) Health Security Threats

(U) Pandemic Influenza

(U) As identified in the 2007 HSTA, DHS/IE judges that an influenza pandemic remains a significant threat to the Homeland and could cause a catastrophic event of national significance.

(U//FOUO) The emergence of a novel, highly transmissible, and virulent illness for which the United States has no countermeasures would pose a serious threat to the Homeland. Influenza is only one of several potentially pandemic-generating classes of disease; however, HPAI (H5N1) remains a likely candidate for initiating a global influenza pandemic. DHS/IE cannot reliably predict if or when this organism will mutate into a variant threatening U.S. public health. The emergence of a noninfluenza pandemic could have similar or even greater consequences than those outlined here.

(U//FOUO) A sustained pandemic with a high fatality rate would cause considerable social disruption to include hundreds of thousands or millions of deaths; degradation of critical infrastructure and essential public and private services because of worker illness or absenteeism; supply chain disruptions to include possible shortages of foodstuffs and other essential goods; and national economic hardship caused by prolonged workspace closures and loss of worker income. Homeland security, law enforcement, and other officials would be challenged to deal with the psychological and social disruptions that would accompany such a catastrophic outbreak.

(U//FOUO) Inadequate global health surveillance systems, increased global travel, and an expectation that people will flee infected areas indicate that localized human outbreaks overseas may be transmitted rapidly to the Homeland with little or no warning.

(U//FOUO) If a pandemic influenza strain emerges, the United States would be unable to prevent its spread into the Homeland, given the speed and volume of modern transportation. The most likely route for an infected individual to enter the United States is by commercial air travel, but if the first appearance of the disease in the Western Hemisphere is in Canada or Latin America, an infected individual could introduce the disease by legally or illegally crossing the U.S. Northern or Southwestern border by land or water.

— (U//FOUO) In 2007, seasonal influenza strains circulating in North America and Europe displayed higher than expected rates of resistance to oseltamivir (Tamiflu), a key antiviral treatment, and H5N1 strains partially resistant to oseltamivir have been isolated from several patients.[81,82] The spread of oseltamivir resistance in seasonal influenza strains may increase the likelihood that an oseltamivir-resistant pandemic influenza strain will emerge.

— (U//FOUO) DHS/IE cannot predict with complete certainty the countries from which HPAI (H5N1) is most likely to translocate into the United States. In 2007, Indonesia and Egypt reported the most cases and fatalities, whereas Pakistan, Laos, Myanmar (Burma), and Nigeria reported their first official cases in 2007.

(U) Indicators of the Emergence of an Influenza Pandemic

— (U) Appearance of a virulent influenza strain that spreads efficiently from human to human.
— (U) Regional medical crises related to disease outbreaks.
— (U) Nation-state actions in response to disease outbreaks.
— (U) Commitment of military forces in response to inability to contain an outbreak.
— (U) Extensive social disorder and unrest in response to an outbreak or collapse of the health infrastructure.

(U) None of these indicators was activated during the past year. A series of animal and human outbreaks of H5N1 avian influenza have occurred overseas. These incidents did not result in widespread human illness, but some localized economic losses occurred as a result of animal culling.

(U) Threats to Critical Infrastructure

(U//FOUO) Cyber Attack

(U//FOUO) The increasing ease of acquiring cyber attack capabilities could lead al-Qa'ida and its affiliates to launch cyber attacks targeting the U.S. economy or critical infrastructure. They could acquire the requisite capabilities by training, purchase, coercion, or outsourcing. Computer network exploitation or computer network attacks could disrupt critical infrastructure systems and "just-in-time" inventory and product distribution systems, crippling key sectors of the U.S. economy.

(U//FOUO) DHS/IE assesses that certain trends have emerged that increase the plausibility of an al-Qa'ida directed or inspired cyber attack that targets the economy during the next three-to-five years. Islamic extremists likely will make progress gaining access to capabilities requisite to conduct cyber attacks.

(U//FOUO) Indicators of Impending Cyber Attack against the U.S. Economy

— (U//FOUO) Evidence of al-Qa'ida supporters gaining sophisticated IT capability or efforts by al-Qa'ida to recruit or otherwise acquire the services of individuals with that capability.
— (U//FOUO) A fatwa or public pronouncement by al-Qa'ida or al-Qa'ida affiliates of the desirability of economic sabotage.
— (U//FOUO) Unexplained use of university network resources by extremist student groups.
— (U//FOUO) Unexplained outages of major IT systems.
— (U//FOUO) Computer network attack trial "probes" increase in frequency.

(U) Threats Posed by Homegrown Extremism and Radicalization

(U//FOUO) Rightwing Terrorist Attacks against the Homeland

(U//FOUO) Rightwing extremists conducting a violent attack of national significance pose the most likely domestic-generated, high consequential threat to the Homeland. This judgment is based on their capabilities and is consistent with judgments reached in the 2007 HSTA. Some rightwing groups possess large weapons caches and are known to conduct paramilitary training; in some cases, members have formal military training.[83,84] A single, large-scale attack like that of the 1995 bombing of the Murrah Federal Building in Oklahoma City is within the capabilities of small cell and lone wolf extremists.

(U//FOUO) Certain government actions and polarizing issues—such as perceived liberalization of immigration laws or stricter firearm regulations—could trigger high-consequence rightwing violence. The 1993 U.S. Government raid on the Branch Davidian compound in Waco, Texas appears to have catalyzed Timothy McVeigh's motivation to bomb the Murrah Federal Building. A change in immigration, gun, or marriage laws; a State or Federal Government action perceived as a violation of civil liberties; or the arrest of a prominent leader could spur large-scale attacks by white supremacists.[85]

(U//FOUO) Rightwing extremists could execute coordinated bombing campaigns. The increasing availability of information on the technology and use of explosive devices has considerably reduced the time it takes to plan and execute coordinated attacks against targets in the United States. Historically, rightwing extremists have targeted government facilities, and law enforcement has succeeded in disrupting many of these plots. If rightwing extremist groups continue to advance their operational security procedures and avoid detection by law enforcement, they could be emboldened to attack such targets and widen their target set to include immigration and naturalization facilities and religious institutions.

(U//FOUO) Alternatively, small, undetected cells and lone wolves could execute copycat attacks producing limited, local physical damage that, because of the sinister nature of such attacks, could extend adverse social or psychological impacts nationwide. Rightwing extremists could carry out attacks similar to the 2002 Washington, D.C. sniper attacks or more recent university shooting incidents. Sniping and shooting sprees are highly effective terror tactics that do not require extensive training or financial resources. Online training, weapons, and other materials that could be used in an attack are readily available, providing small cells or lone wolves the resources to execute such attacks.

— (U) The student gunman who conducted the April 2007 attack on the Virginia Tech campus in Blacksburg, VA was armed with two handguns and at least 400 rounds of ammunition. One of the handguns and much of the ammunition were purchased over the Internet in the two months before the attack

and operational training and exercise was negligible.[86] In the space of 10 minutes, he succeeded in killing 32 of his 49 victims.

(U//FOUO) Indicators of Increasing Rightwing Terrorism

- (U//FOUO) Rightwing groups and individuals issue public calls for a widespread campaign of violence.
- (U//FOUO) Law enforcement detects an increase in the capabilities and activity of paramilitary groups.
- (U//FOUO) An initial attack or attacks occur and groups and individuals coordinate their activities.

(U) **Tracked by:** HSEC-020000-01-05

[1] (U) http://www.state.gov, "Developments in the Iraqi Refugee and Special Immigrant Visa (SIV) Admissions Programs."
[2] (U) http://www.unhcr.org, "UNHCR Meets 2007 Resettlement Referral Target for Iraqi Refugees."
[3] (U) DHS/CBP, ENFORCE, *Special Interest Alien Apprehensions Nation FY 2007*; 7 December 2007.
[4] (U) DHS/CBP, EID, *Border Patrol ASIC Apprehensions FY2007 By Sector and Citizenship*, 3 December 2007.
[5] (U) HIR/HST-0006-08, 1 February 2008.
[6] (U) HIR/HST-0034-07, 20 March 2007.
[7] (U) HIR/CBP-1857-07, 12 September 2007.
[8] (U) HIR/HST-0069-07, 7 December 20007.
[9] (U) HIR/HST-0046-07, 31 July 2007.
[10] (U) State, *Proposed Refugee Admissions for Fiscal Year 2008 Report to the Congress.*
[11] (U) DHS, *2006 Yearbook of Immigration Statistics*, September 2007.
[12] (U) OSC, EUP20071213029001, 13 December 2007
[13] (U) OSC, GMP20071218342001, 16 December 2007
[14] (U) *The Economist*, "Marching as to War," 31 January 2008.
[15] (U) *The Economist*, Intelligence Unit, "No Country for Old Men," 24 January 2008.
[16] (U) NDIC, *National Drug Threat Estimate 2008*, October 2007.
[17] (U) National Seizure System data, December 2007.
[18] (U) Congressional Research Service Report for Congress, *Mexico's Drug Cartels*, 16 October 2007.
[19] (U) *The Economist*, "Marching as to War," 31 January 2008.
[20] (U) *The Economist*, Intelligence Unit, "No Country for Old Men," 24 January 2008.
[21] (U) *Christian Science Monitor*, "Can Mexico's Calderon Stop the Killings?" 2 September 2008.
[22] (U) DHS/CBP, *Assaults against CBP Personnel*, FY 2007 Border Violence Report, 2007.
[23] (U) DHS/CBP, *BorderStat–Violence*, FY 2008 Q1, 2007.
[24] (U//FOUO) NCTC, NSAR 2007-21: Update: 2006 SIA Trends Reveal Vulnerabilities along Route to US," 11 May 2007.
[25] (U//FOUO) Joint Reserve Intelligence Center, Foreign Military Studies Office, *Islam in a Sombrero Part I Southern Mexico*, 28 February 2004.
[26] (U) ADL, Terrorism Update: "Canada and Terrorism," 24 January 2004.
[27] (U) *National Post*, "First Guilty Verdict in Toronto 18 Trials," 25 September 2008.
[28] (U) *Online Journal*, "Feels Like June 2, 2006, All over Again," 7 April 2008.
[29] (U//FOUO) DHS, *Homeland Security Assessment*, "U.S.–Mexico Border: Record Number of Underground Tunnels Discovered in 2007," 19 February 2008.
[30] (U) *The Washington Post*, "Drug Traffic beneath the Waves," 6 February 2008.
[31] (U) *La Jornada*, "Mexico: Drug-Laden Submarine Found Off Oaxaca Coasts Said Russian Made," 18 July 2008.
[32] (U) *Notimex*, "Mexico: Submersible Carrying Drugs Caught Off Oaxaca Coast," 17 July 2008.
[33] (U) National Drug Intelligence Center, "Washington/Baltimore High Intensity Drug Trafficking Area Drug Market Analysis 2008," June 2008.
[34] (U) IIR 4 214 0308 08, 23 October 2007.
[35] (U) KCCI News, Des Moines, IA, November 2, 2007.
[36] (U) http://www.who.int, "World Health Organization."
[37] (U) *Emerging Infectious Diseases*, Vol. 13, No. 9, "Detecting Human-to-Human Transmission of Avian Influenza A (H5N1)," September 2007.
[38] (U) *Emerging Infectious Diseases*, Vol. 12, No. 1, "H5N1 Outbreaks and Enzootic Influenza," January 2006.
[39] (U) *PLoS Pathogens* Vol. 3, No. 10, "Growth of H5N1 Influenza A Viruses in the Upper Respiratory Tracts of Mice," October 2007.
[40] (U) http://www.beta.deq.virginia.gov, Bendfeldt, Peer, and Flory, "Lessons Learned from Avian Influenza Outbreaks in Virginia 1983 and 2002."
[41] (U) http://www.aphis.usda.gov, "Animal and Plant Health Inspection Service."
[42] (U) http://www.medscape.com, "Medscape Infectious Diseases."
[43] (U) *The New York Times*, "Test Shows Ease of Buying Bomb Parts," 13 September 2006.

[44] (U) *The Washington Post*, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," 19 January 2008.
[45] (U) *The Washington Post*, "Wall Street Reports Increase in PC Intrusions in '07," 22 February 2008.
[46] (U) *The Washington Post*, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," 19 January 2008.
[47] (U) IIR 4 230 1643 08, 23 June 2008.
[48] (U) http://www.telegraph.co.uk, "Gangs Target MySpace to Recruit Members."
[49] (U) *Leaderless Jihad: Terror Networks in the Twenty-First Century*, (Pennsylvania, University of Pennsylvania Press, 2008).
[50] (U) *Leaderless Jihad: Terror Networks in the Twenty-First Century*, (Pennsylvania, University of Pennsylvania Press, 2008).
[51] (U//FOUO) DHS, *Homeland Security Intelligence Assessment*, "Online Extremist Propagandists Target U.S. Muslims," 5 November 2007.
[52] (U//FOUO) DHS, *Special Assessment*, "The Domestic Terrorism Threat: Lone Wolves, Small Cells, and Leaderless Resistance," 5 July 2005.
[53] (U) *Igniting the Revolution: An Introduction to the Earth Liberation Front*, (Oregon, North American Earth Liberation Front Press Office, 2001).
[54] (U) IIR 4 201 0047 06, 8 October 2005.
[55] (U//FOUO) DHS, *Special Assessment*, "The Domestic Terrorism Threat: Lone Wolves, Small Cells, and Leaderless Resistance," 5 July 2005.
[56] (U//FOUO) DHS, "*Racist Skinheads: A Potential Terrorist Threat*," 3 November 2006.
[57] (U) IIR 4 201 0297 05, 28 October 2004.
[58] (U) SPL, Intelligence Report, "Terror, American Style," Spring 2004.
[59] (U) U.S. Department of Justice Press Release, "Federal Grand Jury Charges Man Who Possessed Cyanide," 17 June 2008.
[60] (U) IIR 4 201 2851 07, 10 August 2007.
[61] (U) IIR 4 201 4757 07, 9 September 2007.
[62] (U) Senate Judiciary Committee, "Statement of John E. Lewis Deputy Assistant Director Counterterrorism Division FBI before the Senate Judiciary Committee," 18 May 2004.
[63] (U) http://www.animalliverationpressoffice.com.
[64] (U) http://www.elfpressoffice.org.
[65] (U) ADL, "Dangerous Convictions: Extremist Recruitment in America's Prisons," 2 July 2002.
[66] (U) IIR 4 214 2107 08, 29 November 2007.
[67] (U) Speech by Robert S. Mueller, III, *Council of Foreign Relations*, 28 September 2007.
[68] (U) U.S. v. Ahmed, (N.D. G.A.), No. 1:06-CR-147-CC, Indictment Filed 19 July 2006.
[69] (U//FOUO) FBI, *The Mohajroon Bulletin Board: An Online Window Into Jihadist Propaganda and Operational Planning*, 22 August 2007.
[70] (U) MAGLOCLEN Network, "Paroled Michigan Militia Leader Posting Training Videos to Youtube," November 2007.
[71] (U) http://www.animalliberation.net.
[72] (U) "Setting Fires with Electric Timers: An Earth Liberation Front Guide," May 2001.
[73] (U//FOUO) DHS, *Homeland Security Intelligence Assessment*, "Online Extremist Propagandists Target U.S. Muslims," 5 November 2007.
[74] (U//FOUO) DHS, *Homeland Security Intelligence Assessment*, "Recent Al-Qa'ida Propaganda May Resonate with U.S. Minorities," 21 August 2007.
[75] (U) IIR 4 201 1694 07, 9 February 2007.
[76] (U) IIR 4 201 1711 07, 10 February 2007.
[77] (U) *The Washington Post*, "Raul Castro Succeeds Fidel as President of Cuba," 24 February 2008.
[78] (U) OSC, LAP 20071205361002, 5 December 2007.
[79] (U) http://news.bbc.co.uk, "Stepping into Big Brother's Shoes?"
[80] (U) http://news.bbc.co.uk, "Stepping into Big Brother's Shoes?"
[81] (U) http://www.cdc.gov, "Avian Influenza."
[82] (U) http://www.cidrapsummit.net, "Avian Influenza."
[83] (U) IIR 4 201 2528 08, 28 January 2008.

[84] (U) IIR 4 201 4757 07, 9 September 2007.
[85] (U) HIR/DHS-0003-07, 5 March 2007.
[86] (U) Report of the Virginia Tech Review Panel, "Mass Shootings at Virginia Tech April 16, 2007," August 2007.

(U//FOUO) Appendix: Consequence Ranking Table

Consequence Level					
	0 None or Negligible	**1 Minor**	**2 Moderate**	**3 Significant**	**4 Catastrophic or Severe**
Loss of Life *(Attack likely to cause:)*	No fatalities.	Less than 100 fatalities.	More than 100 fatalities.	More than 1,000 fatalities.	More than 10,000 fatalities
Economic Damage *(Costs of the attack are estimated as:)*	Less than $100 million.	In the range of $100 million to $1 billion.	In the range of $1 to $10 billion. *(11 September 2001 attack on the Pentagon)*	In the range of $10 to $100 billion. *(11 September 2001 attack on the World Trade Center)*	In excess of $100 billion *(nuclear attack)*
Psychological Impact	No major change in population behavior; no effects on social functioning.	Occasional or minor loss of nonessential social functions in a circum-scribed geographical area.	Loss of many Nonessential social functions in a circum-scribed geographical area.	Dysfunctional behavior and disruption of important social functions for a sustained period.	Loss of belief in government and institutions; widespread dis-regard for official instructions; widespread looting and civil unrest.