(U) 2011 NATIONAL RISK PROFILE

Homeland Infrastructure Threat and Risk Analysis Center

Office of Infrastructure Protection

National Protection and Programs Directorate

U.S. Department of Homeland Security

July 2011

(U) Contents

(U) Executive Summary: National Risk Landscape

(U) The 2011 National Risk Profile describes the risks facing the Nation's critical infrastructure that must be managed by the Department of Homeland Security and its partners. It is designed to help policy and budgetary decisionmakers and critical infrastructure partners understand the critical infrastructure risk landscape and inform their risk management decisions. It does not address all potential risks, but it does address those risks created by threats and vulnerabilities that may cause significant consequences.

(U) Every day, the Nation faces myriad risks—naturally occurring and manmade (intentionally and unintentionally introduced)—that affect public health, safety, and security. The risk taxonomy below (see Figure 1) illustrates a number of those important risks facing critical infrastructure in 2011 and beyond, although it could be expanded to include many more.

(U) Nine national, cross-cutting risks have been identified in the 2011 National Risk Profile in consultation with critical infrastructure protection and resilience partners. These prevalent risks to the critical infrastructure are grouped in accordance with this risk taxonomy: (1) naturally occurring risks (space weather, extreme weather, and pandemic disease); (2) unintentionally introduced manmade risks (industrial disaster, aging infrastructure, and economic instability); and (3) intentionally introduced manmade risks (terrorism, border security, and cyber disruption). Critical infrastructure risks to each of the 18 critical infrastructure sectors and 10 federally administered regions have also been provided. There may be cases where the national risks may not be as great to a particular region or sector but still create cross-cutting risk. The national, regional, and sectoral perspectives used to evaluate these risks add dimensionality and the interdependent nature of the critical infrastructure adds depth. Looking at the prevalence of threats, vulnerabilities, consequences, and the overall risk composed of these elements for the critical infrastructure sectors indicates the following for the overall National Risk Landscape:

- (U) The Transportation Systems Sector, Energy Sector, Food and Agriculture Sector, and Commercial Facilities Sector (in order) are potentially most affected by national cross-cutting risks and risks characteristic of individual federally administered regions;
- (U) Cyber disruption, terrorism, natural disasters, insider threats, and supply chain vulnerabilities (in order) potentially contribute most to critical infrastructure risks;

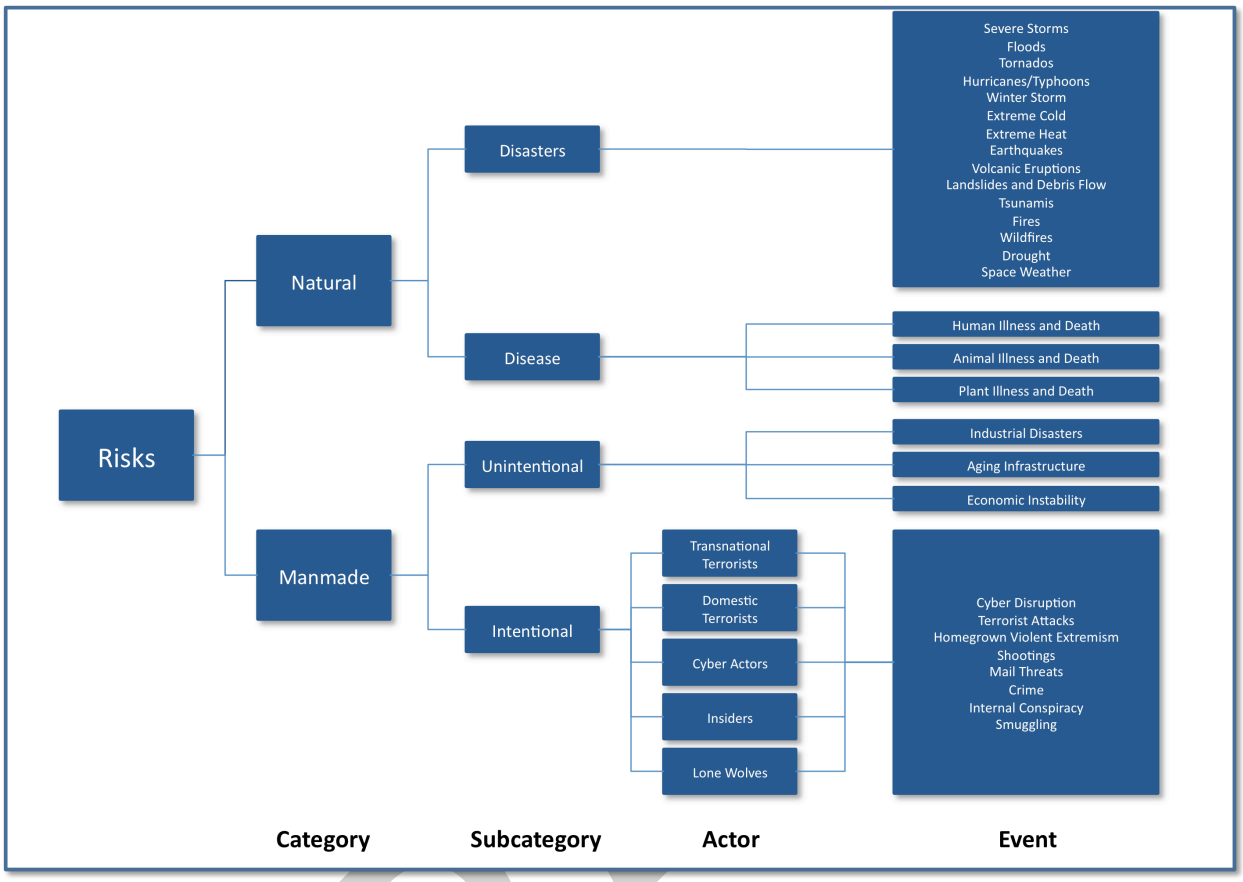
- (U) Severe storms, flooding, hurricanes/typhoons, and tornadoes (in order) potentially create the most weather-related risk for the critical infrastructure sectors and regions; and

- (U) The interdependent nature of the critical infrastructure sectors means that even those sectors that are at lesser risk may be affected when other sectors at higher risk are damaged or destroyed.

(U) Policy and budgetary decisionmakers and critical infrastructure partners are challenged in their efforts to mitigate critical infrastructure risk by the large number and complexity of risks that could potentially affect their areas of responsibility. By identifying the most prevalent risks to the critical infrastructure and the elements that contribute most to regional and sectoral risks, this National Risk Profile may offer guidance to those decisionmakers regarding resource allocation and priorities.

(U) The 9/11 Commission Report noted that the inability to foresee possibilities that might occur in the future was among the key contributors in the failure to prevent the attack on September 11, 2011. Although the Commission was referring to terrorism, the same can be said regarding all of the risks outlined here. Forecasting is part of the planning paradigm, but such planning is an activity that is often sacrificed when trying to do more with less. Even when planning does occur, it may only address first-order events, such as an earthquake occurring in a particular geographic area and affecting a particular critical infrastructure sector. Second-order and other events, such as an ensuing tsunami and the impact of that tsunami on nuclear power plants, may not be identified in advance. If they are not identified in advance, the necessary plans will not be put in place, response to such complex emergencies will be conducted without the benefit of already identified actions. The inability to foresee possibilities and subsequently respond to the crises created by these possibilities contributes directly to critical infrastructure risk. The National Risk Profile seeks to identify risk, in part, through forecasting and other methods to imagine possibilities.

(U) As with any landscape, over the course of time, changes occur. They can alter the landscape, increase visibility, and clarify the horizon. As the risks and/or our understanding of the risks in the National Risk Profile change, so may parts of the National Risk Profile and the National Risk Landscape derived from it. Notwithstanding this potential for change, the 2011 National Risk Profile addresses risks that impact the Nation's critical infrastructure now and are expected to be pose risks to the critical infrastructure in the future. This allows planners to address more than just today's risk landscape.



(U) Figure 1: Risk Taxonomy

(U) Key Findings

(U) Naturally Occurring Risks

- **(U) Space Weather Risks** – The next peak of solar activity should occur by 2013. Solar activity—particularly solar storms—produces the direst consequences and contributes greatly to critical infrastructure risk, especially since it potentially disrupts fundamental operating systems. Geographically, the entire United States is at risk from space weather, with those States in the upper latitudes at greater risk. The space weather risk is greatest for the Energy Sector, as well as the Communications Sector and Transportation Systems Sector.

- **(U) Extreme Weather Risks** – Although coastal hurricanes, tropical storms, and tsunamis are the most costly extreme weather events, those caused by extreme hot and cold temperatures, as well as severe storms and the flooding associated with them occur much more frequently. These commonly occurring extreme weather events contribute most significantly to critical infrastructure risk by potentially reducing operability temporarily or permanently. Geographically, the entire United States is at risk from extreme weather. Extreme temperatures create the greatest risk for the Communications Sector, Energy Sector, Food and Agriculture Sector, Healthcare and Public Health Sector, Transportation Systems Sector, and Water Sector.

- **(U) Pandemic Disease Risks** – The most threatening pandemic diseases are caused by highly pathogenic microorganisms for which humans, animals, or plants have not developed immunity and for which medications or treatments do not already exist or cannot be developed quickly, manufactured easily, or distributed efficiently. Risk for the critical infrastructure is due to difficulty in characterizing pandemic disease in advance, reduced available workforce, and increased demand to manage the pandemic and its impacts. Geographically, the entire United States is at risk from pandemic disease. Pandemic disease creates the greatest risk for the Healthcare and Public Health Sector and Emergency Services Sector (in the case of pandemics affecting humans) and the Food and Agriculture Sector (in the case of pandemics affecting animals and plants), followed by the Banking and Finance Sector, Emergency Service Sector, Information Technology Sector, Transportation Systems Sector, and Water Sector. If demand for services is great enough, the Food and Agriculture Sector (in the case of pandemic animal disease) and the Healthcare and Public Health Sector (in the case of pandemic human disease) could cease to function entirely.

(U) Unintentionally Introduced Manmade Risks

- **(U) Industrial Disasters Risks** – Aside from the potential for catastrophic consequences associated with industrial disasters, this risk for the critical infrastructure is due to the inability of industry to do more with less and the inability to recognize unusual circumstances in industrial design or operation. Geographically, industry throughout the entire United States is at risk from industrial disasters. These human factors create the greatest risk of industrial disaster for the Chemical Sector Critical Manufacturing Sector Defense Industrial Base Sector Energy Sector Food and Agriculture Sector Nuclear Reactors, Materials, and Waste Sector Transportation Systems Sector and Water Sector.

- **(U) Aging Infrastructure Risks** – Unusable, ineffectual, and deteriorating critical infrastructure, as well as the potential for exploitation of these vulnerabilities, increase risk. Risk for the critical infrastructure is due to the inadvertent introduction of flaws, reduced inspection and maintenance workforce, and insufficient investment. Geographically, the entire United States is at risk from aging infrastructure. Aging will affect all critical infrastructure sectors and ultimately reduce or erode their capacity and lifetimes in unexpected and unpredicted ways. Attempts to counteract ill effects vary by critical infrastructure type and associated funding. Economic effects could also result from aging infrastructure, as the lack of spending on critical infrastructure throughout the United States may cause the Nation to lose competitiveness in the global market.

- **(U) Economic Instability Risks** – An unstable economy can suffer from reduced government spending, high unemployment, inflation, and/or pronounced business cycles that reduce private sector spending. Lack of public and private sector spending and unemployment contribute most to risk for the critical infrastructure, making it less reliable, safe, and secure. Geographically, the entire United States is at risk from economic instability. Those sectors that that are considered critical parts of the national security apparatus (such as the Defense Industrial Base Sector, Government Facilities Sector, and parts of the Transportation Systems Sector) may fare better, but an unstable economy could increase risk for all critical infrastructure sectors.

(U) Intentionally Introduced Manmade Risks

- **(U//FOUO) Terrorism Risks** –Every critical infrastructure sector is potentially at risk for terrorism. Decentralization of terrorist groups increases risk throughout the Nation and its critical infrastructure. However, some sectors are at greater risk due

to greater expressed interest on the part of terrorists, greater potential consequences, and/or lower perceived security postures. Geographically, the entire United States is at risk from terrorism, although some locations are at greater risk than others. The Commercial Facilities Sector, Government Facilities Sector, Banking and Finance Sector, and Transportation Systems Sector face greatest risk due to their public accessibility, the high density of people in enclosed areas, and the potential for psychological impacts beyond an initial attack. The Chemical Sector, Dams Sector, Food and Agriculture Sector, and Water Sector are at greater risk due to the potential for large consequences. The Commercial Facilities Sector and Transportation Systems Sector are at greatest risk due to their vulnerability to small-scale operations. Although the use of IEDs contributes to risk for all critical infrastructure sectors, recent plots and events indicate that the Postal and Shipping Sector and Transportation Systems Sector continue to be at particular risk. Economically important critical infrastructure in the United States also remains a possible target.

- **(U) Border Security Risks** - Threats coming across and vulnerabilities at any part of the border create risk for the critical infrastructure that is located at the border and the critical infrastructure that relies on supplies that have to cross the border. The greatest border security risks to critical infrastructure are due to lack of personnel security, importation and use of counterfeit materials, and exploitation of vulnerabilities where critical infrastructure is located at the border. The large span of some borders contributes to these problems and provides greater access by criminals and terrorists. However, geographically, the entire United States is at risk for lack of border security. Lack of effective border security creates the greatest risk for the Banking and Finance Sector, Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Energy Sector, Food and Agriculture Sector, Healthcare and Public Health Sector, Information Technology Sector, Postal and Shipping Sector, Transportation Systems Sector, and Water Sector.

- **(U) Cyber Disruption Risks** – The critical infrastructure community faces new challenges regarding cyber disruptions. The greatest cyber disruption risks are due to attacks on the cyber infrastructure and continuous adaptation of the threat. Geographically, the entire United States is at risk for cyber disruption. Cyber disruption creates the greatest risk for the Banking and Finance Sector; Commercial Facilities Sector; Communications Sector; Critical Manufacturing Sector; Dams Sector; Emergency Services Sector; Energy Sector; Food and Agriculture Sector; Government Facilities Sector; Healthcare and Public Health Sector; Transportation

Systems Sector; Nuclear Reactors, Materials, and Waste Sector; Postal and Shipping Sector; and Transportation Systems Sector.

(U) Sector Risks

- **(U) Banking and Finance** – The sector faces current and ongoing risks from cyber attacks, insider wrongdoing, pandemic disease, and large-scale physical attacks.
- **(U) Chemical** – The sector faces current and increasing risks owing to the vulnerability of network-based control systems, insider threats, terrorist threats, and natural disasters and accidents.
- **(U) Commercial Facilities** – The sector faces ongoing and increasing risks from bombing; active shooters; and terrorist attacks using chemical, biological, radiological, or nuclear weapons or agents.
- **(U) Communications** – The sector faces ongoing risks from cyber disruption, insider threats, and space weather.
- **(U) Dams** – The sector faces current and increasing risks from natural hazards, the use of explosives by determined aggressors, and aging infrastructure.
- **(U) Defense Industrial Base** – The sector faces risks from cyber disruption and loss of supply chain integrity.
- **(U) Emergency Services** – The sector faces risks from a lack of standardized and common communications resources, dependence on transportation for the movement of personnel, supplies, and other resources, pandemic disease, and from terrorist attacks using hazardous materials and/or chemical, biological, radiological, or nuclear agents.
- **(U) Energy** – The sector faces current, continuing, and increasing risks from cyber attacks, physical attacks, and natural hazards.
- **(U) Food and Agriculture** - The sector faces ongoing and increasing risks from food contamination through often unanticipated transport mechanisms, disease and pests, and severe weather.
- **(U) Government Facilities** – The sector faces current and ongoing risks from terrorist attacks, cyber security breaches, and ineffective security personnel procurement and oversight.

- **(U) Healthcare and Public Health** – The sector faces current and ongoing risks from global supply chain disruptions, theft and exploitation of medical goods and confidential medical information, and pandemic disease.
- **(U) Information Technology** – The sector faces current and ongoing risks from cyber disruptions and supply chain vulnerabilities.
- **(U) National Monuments and Icons** – The sector faces current and increasing risks from terrorist attacks.
- **(U) Nuclear Reactors, Materials, and Waste** – The sector faces current and ongoing risks from physical incidents, cyber intrusions, insider threats, theft and diversion of materials, severe weather, and supply chain vulnerabilities.
- **(U) Postal and Shipping** – The sector faces current and ongoing risks owing to the openness of the sector, mail-based threats, and attacks on modes of transportation.
- **(U) Transportation Systems** – The sector faces current and ongoing risks from terrorism, sector openness, and interdependencies with other critical infrastructure sectors.
- **(U) Water** – The sector faces current and ongoing risks from contamination, natural hazards, aging infrastructure, and physical and cyber attacks directed against this sector and other sectors upon which it is dependent.

(U) Regional Risks

- **(U) Region I** – The region will continue to experience risks from severe winter weather, hurricanes, and other storms that can cause flooding, and risks to the Energy Sector and Transportation Systems Sector in particular.
- **(U) Region II** – The region will continue to experience risks from severe storms and risks to the Banking and Finance Sector and Transportation Systems Sector in particular.
- **(U) Region III** – The region will continue to experience risks from floods, hurricanes, severe storms, snow, and tornadoes, and risks to the Government Facilities Sector and Transportation Systems Sector in particular.

- **(U) Region IV** – The region will continue to experience risks from hurricanes, tornadoes, flooding, ice storms, wildfires, and earthquakes due to the New Madrid Seismic Zone, and risks to the Commercial Facilities Sector and Chemical Sector in particular.

- **(U) Region V** – The region will continue to experience risks from flooding, severe storms, and tornadoes, and risks to the Food and Agriculture Sector and Transportation Systems Sector in particular.

- **(U) Region VI** – The region will continue to experience risks from coastal storms, hurricanes, severe ice storms, and severe storms, and risks to the Chemical Sector, Commercial Facilities Sector, and Energy Sector in particular.

- **(U) Region VII** – The region will continue to experience risks from floods, severe storms, tornadoes, and earthquakes due to the New Madrid Seismic Zone, and risks to the Chemical Sector and Food and Agriculture Sector in particular.

- **(U) Region VIII** – The region will continue to experience risks from severe storms and events that cause flooding, and landslides, and risks to the Dams Sector and Water Sector in particular.

- **(U) Region IX** – The region will continue to experience risks from earthquakes, severe storms, typhoons, and wildfires, and risks to the Commercial Facilities Sector and Transportation Systems Sector in particular.

- **(U) Region X** – The region will continue to experience risks from earthquakes, landslides, severe storms, tornadoes, volcanic eruptions, and wildfires, and risks to the Energy Sector and Transportation Systems Sector in particular.

(U) Introduction

(U) The 2011 National Risk Profile describes the risks facing the Nation's critical infrastructure that must be managed by the Department of Homeland Security and its partners. It is designed to help policy and budgetary decisionmakers and critical infrastructure partners understand the critical infrastructure risk landscape and inform their risk management decisions. It does not address all potential risks, but it does address those risks created by threats and vulnerabilities that may cause significant consequences.

(U) The 2011 National Risk Profile looks forward at risks to critical infrastructure and will be the basis for reporting back in the 2012 National Critical Infrastructure Protection Annual Report and the 2012 Sector Annual Report for each critical sector. Those documents will, in part, assess how the risks described in this document were managed in 2012. These risks will also be considered and addressed in the triennial Critical Infrastructure Risk Management Plan. Using qualitative and quantitative analysis and the best information available from our partners, the 2011 National Risk Profile looks into the future. It will be updated annually. While there are no perfect predictions, the National Risk Profile helps decisionmakers address the risks of tomorrow with the leadership and resources of today.

(U) Purpose

(U) The Homeland Security Act of 2002 requires the Secretary of Homeland Security to report annually to Congress on: (1) risks to the Nation's critical infrastructure; and (2) the regulatory and voluntary measures taken to manage those risks. The Department of Homeland Security Office of Infrastructure Protection began the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI) in 2010 to strengthen the link between the National Risk Profile, the National Critical Infrastructure Protection Annual Report, and the Critical Infrastructure Risk Management Plan so that planning and resource allocation would be based upon risk-informed metrics. These three documents address congressionally mandated annual reporting requirements. They also serve as the foundation for critical infrastructure protection strategic and budgetary planning, ensuring that tactical resources roll-up into a strategic direction that is based upon the measurable management of defined risks as agreed to by the interagency and private partners.

(U) Scope

(U) The 2011 National Risk Profile addresses past and current risks. It includes information regarding the threat to, vulnerability of, and consequences for the critical infrastructure sectors and uses that information to look forward at risks to critical infrastructure.[a]

(U) Methodology

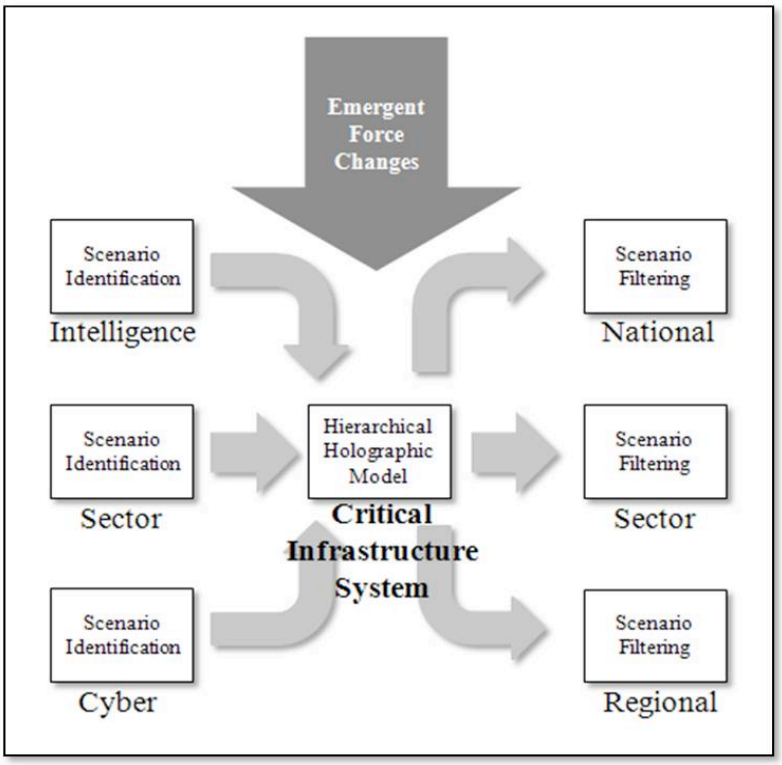
(U) Partnership engagement was critical to each methodological step used to develop the 2011 National Risk Profile. Critical infrastructure and resilience partners clearly articulated what the National Risk Profile needed to provide them in the way of decision support. These partners, as well as analysts throughout the Department of Homeland Security and the Federal Government, were engaged, providing qualitative and quantitative data for the analysis supporting the 2011 National Risk Profile. Outreach was conducted through the Sector Coordinating Councils; Government Coordinating Councils; Federal Senior Leadership Council; Regional Consortium Coordinating Council; State, Local, Tribal, and Territorial Government Coordinating Council; Regional Protective Security Advisors, Private Sector Cross-Sector Council, Federal Departments and agencies; and other relevant and interested organizations. Data were also drawn from sources already produced by our partners, such as sector risk assessments and Federal Emergency Management Agency hazard reports. Our partners within the Intelligence Community were also asked to identify sector-specific threats by actor and attack method.

(U) Sector-specific plans were analyzed to produce a hierarchical holographic model.[b] The Intelligence Community, critical infrastructure partners, and the cyber community identified risk-related scenarios that were applied to the model. Leadership within the Department of Homeland Security Office of Infrastructure Protection identified emergent forces that were also applied to the model. These scenarios were filtered at the national, regional, and sectoral levels. Statistically significant natural hazards data were identified. The results of the filtering and statistical identification were combined and resulted in the analysis of the critical infrastructure system. The diagram below (see Figure 2) illustrates this methodology.

[a] (U) "Historians are fond of saying that the study of the past can help us to understand the future. Futurists agree, and point out that all our ideas about the future necessarily come from the past, not the future itself, for the very simple reason that the future, by definition, has never existed. What has happened in the past is our only source of guidance to what may happen in the future." [Cornish, E., *The Study of the Future: An Introduction to the Art and Science of Understanding and Shaping Tomorrow's World*, Washington, DC: World Futures Society, 1977: p. 103]

[b] Hierarchical Holographic Modeling is a structured approach to look at complex systems from multiple perspectives.

UNCLASSIFIED



(U) Figure 2: 2011 NRP Methodological Approach

(U) Hierarchical holographic modeling trend analysis, research studies of changes over time, statistical analysis, scenario development, structuring, filtering, and analysis and the identification of relevant, probable, and possible futures were based on information provided by our partners regarding previous, current, and emerging threats, vulnerabilities, and consequences.

(U) Given the need to understand risk and identify risk futures for the Nation, it was not possible to depend entirely on quantitative data. Where sufficient data existed, quantitative methods (e.g., trend analysis, environmental scanning, and extrapolation) were used. Where data were insufficient, subjective methods to elicit judgments were used (e.g., solicitation of expert opinion and structured analogies).

(U) Naturally Occurring Risks

(U) Although disaster-related fatalities have generally declined, economic recovery costs have at least doubled every decade, due to increasing population and physical critical infrastructure density throughout the Nation—particularly along the coastlines.[1] Significant investments are not expected to be made over the next 25 years in technology to control the weather and other such naturally occurring phenomena. Therefore, those charged with protecting critical infrastructure must plan for the continued occurrence of natural hazards, err on the side of caution, and assume equal or greater severity or impact. Three naturally occurring risks have been identified in the 2011 National Risk Profile as having potentially significant impact in the critical infrastructure context: space weather risks, extreme weather risks, and pandemic disease risks.

(U) Space Weather Risks

(U) Space weather[c] is always present and is characterized by a variety of activities that produce a spectrum of consequences. Solar activity—particularly solar storms—produces the direst consequences and contributes most significantly to critical infrastructure risk. Geographically, all of the United States is at risk from space weather, with those in the upper latitudes at greater risk.[2]

(U) Solar activity cycles have extremes occurring approximately every 11 years.[3] After a relatively calm period,[4] the sun started becoming more active at the beginning of 2011 and is expected to become increasingly active into 2013,[5] when the next solar maximum occurs[6] and the cycle begins again. However, the next extreme space weather event could occur before 2013. Space weather risk is expected to increase at least until 2013.

(U) Extreme space weather events that create widespread blackouts and irreparable equipment damage[7] could affect millions of people,[d] cost the Nation billions of dollars,[e]

[c] (U) Space weather is composed of severe disturbances of the upper atmosphere and the near-Earth space environment that are driven by the magnetic activity of the Sun. [Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, *Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report*, Washington, DC: National Academies Press, 2008: p. 1, www.nap.edu/catalog/12507.html, accessed 12 April 2011]

[d] (U) For example, a solar storm in 1989 caused northeastern Canada's Hydro-Quebec power grid to collapse within 90 seconds, leaving millions of people without electricity for up to nine hours. [Kappenman JG, Zanetti, LJ, and Radasky, WA, *Geomagnetic Storms Can Threaten Electric Power Grid*, EV World, accessed at http://evworld.com/article.cfm?storyid=246 on April 22, 2011]

[e] (U) If a space weather event occurs that is even slightly more severe than the geomagnetic storm of 1980, there could be a $36 billion loss in gross domestic product. Also, "other assessments placed the 1989 and 1991 geomagnetic storm effects in a category equivalent to Hurricane Hugo and the San Francisco earthquake in their relative impact on the reliability of the electric power grid." [Kappenman JG, Zanetti, LJ, and Radasky, WA, *Geomagnetic Storms Can Threaten Electric Power Grid*, EV World, accessed at http://evworld.com/article.cfm?storyid=246 on April 22, 2011]

and take years to achieve full recovery.[f] These large consequences contribute greatly to risk. However, lesser space weather activities also contribute to ongoing risk. For example, solar activity disrupted communication satellites in June 2011, but the effect was manageable.[8] Although it is not yet possible to accurately predict the severity of solar storms and other solar activity, the length of the solar cycles (11 years) has been documented and the effects of solar activity can be forecasted.[g]

(U) Space weather risk is greatest for the Energy Sector[h] due to its susceptibility to the magnetic disruptions created by solar storms. The Communications Sector and the Transportation Systems Sector also use technology that is susceptible to magnetic disruption and are therefore also at risk. This risk is proportional to the amount of such technology these and other critical infrastructure sectors possess and how much they depend upon it.

(U) Extreme Weather Risks

(U) Although coastal hurricanes, tropical storms, and tsunamis are the most costly extreme weather events,[i] those caused by extreme hot and cold temperatures and severe storms (and the flooding associated with them) occur much more frequently.[j] These commonly occurring extreme weather events contribute most significantly to critical infrastructure risk. (Extreme weather risks specific to geographic areas of the United States can be found in the Regional Risk section below.)

(U) Extreme temperatures increase risk by affecting materials, humans, animals, and plants. Higher and lower temperatures over prolonged periods of time increase risk to the critical infrastructure, causing elements to break and cease to function. For example, pipelines that freeze and then rupture place the Transportation Systems Sector at risk;[9] when temperatures get too high,[k] people, animals, and plants may die, placing the Food and Agriculture Sector and the Healthcare and Public Health Sector at

[f] "(U) The 1859 storm—known as the "Carrington Event" after astronomer Richard Carrington, who witnessed the instigating solar flare—electrified transmission cables, set fires in telegraph offices, and produced Northern Lights so bright that people could read newspapers by their red and green glow. A report by the National Academy of Sciences found that if a similar storm occurred today, it could cause $1 to 2 trillion in damages to society's high-tech infrastructure and require 4 to 10 years for complete recovery. For comparison, Hurricane Katrina caused "only" $80 to 125 billion in damage." [National Aeronautics and Space Administration, *New Solar Cycle Predicted*, http://science.nasa.gov/science-news/science-at-nasa/2009/29may_noaaprediction/, accessed April 25, 2011]

[g] (U) The NOAA Space Weather Prediction Center conducts such forecasting. [http://www.swpc.noaa.gov/alerts/index.html]

[h] Particularly the Electricity Subsector.

[i] (U) Coastal hurricanes, tropical storms, and tsunamis account for the greatest cost—by approximately four times—than other naturally occurring events.

[j] (U) Extreme temperatures refer to what are most commonly known as heat and cold waves. A severe thunderstorm is any storm that produces one or more of the following elements: (1) a tornado; (2) damaging winds or winds measured at 50 knots (approximately 58 miles per hour) or more; or (3) hail one inch in diameter or larger. [National Weather Service, "SPC and its Products," www.spc.noaa.gov/misc/about.html, accessed March 31, 2011]

[k] (U) Extreme temperatures are underscored by NOAA tracking of temperature anomalies. For example in its 2010 annual report, NOAA notes that "each of the 10 warmest average global temperatures recorded since 1880 have occurred in the last 13 years. The warmest years on record are 2005 and 2010." [NOAA, *National Climatic Data Center NCDC 2010 Annual State of the Climate Report,* www.noaanews.noaa.gov/stories 2011/20110112_globalstats_sup.html, accessed June 29, 2011]

risk. Urbanization exacerbates temperature extremes and increases the risk to critical infrastructures characteristic of, connected to, or located within these areas.[10] Critical infrastructure risk increases as urbanization increases, an important consideration as it is expected that by 2030, 60 percent of the world's landmass is expected to be urbanized.[11]

(U) Severe storms and flooding are expected to continue to account for the largest number of Presidential disaster declarations annually[12] and the largest percentage of disaster declarations in every Federal region in the United States.[13] Critical infrastructure is at risk when severe storms and flooding overwhelm and disable large parts of the critical infrastructure simultaneously. These events could also increase the risk to critical infrastructure in urban areas in particular,[14] because more people, critical infrastructure, and resources are concentrated there.

(U) Extreme temperatures along with drought create the greatest risk for the Food and Agriculture Sector and the Healthcare and Public Health Sector because extreme temperatures result in crop destruction, injuries, and death,[15] as well as greatly reduced agricultural production, increased wildfires, and aggravated disease conditions. Extreme temperatures increase risk to those critical infrastructure sectors for which temperature control is both necessary and difficult to achieve in order to ensure that their infrastructure elements function properly. This risk is greatest for the Communications Sector, Energy Sector, Transportation Systems Sector, and the Water Sector.

(U) Severe storms and flooding create the greatest risk for the Dams Sector (as dams and associated infrastructure, such as levees, could be overwhelmed by flooding), Energy Sector (because electrical storms in particular affect energy production), Food and Agriculture Sector (as these events greatly affect crops and agriculture production), Transportation Systems Sector (as it becomes increasingly difficult to transport anything in any mode if the sector is affected by storms and flooding), and Water Sector (when flooding exceeds the Water Sector's ability to ensure water sources are clean and free of pollutants).

(U) Pandemic Disease Risks

(U) The most threatening pandemic diseases[l] are caused by highly pathogenic microorganisms[m] for which humans, animals, or plants (depending on the disease) have

[l] (U) Pandemic diseases are defined as those diseases that spread throughout the world. The ability of a disease to create a pandemic depends on the ability of the disease to spread quickly, the immunity that individuals and populations have to the disease, the availability of medications and equipment to treat the disease, the ability of nations and organizations to take action to stop the spread of the disease, and whether the disease produces serious health effects. Although pandemic influenza and other types of pandemics (e.g., colds) occur every year, they are usually of low virulence and do not result in large numbers of very sick and dead.

[m] U) Three types of highly pathogenic pandemic disease create the greatest risks: (1) those caused by diseases that are ever-present and that continuously and quickly mutate, for which new or modified medicines and treatments must be developed with each significant mutation because the human population has little or no immunity (e.g., influenza); (2) those caused by relatively

not developed immunity,[16] and for which medications or treatments do not already exist or cannot be developed quickly, manufactured easily, or distributed efficiently.[n] Risk for the critical infrastructure is due to difficulty in characterizing pandemic disease in advance, reduced available workforce, and increased demand to manage the pandemic and its impacts.

(U) Diseases that cause pandemics, such as influenza, are not easy to characterize in advance, as it is difficult to ascertain which strains of the disease will be circulating in successive years, how these viruses will mutate, and from where a pandemic will arise. The exact nature of the threat of pandemic influenza[o] and other diseases is, therefore, difficult to identify, resulting in inaccurate determinations of risk. However, history has shown that individuals and groups are vulnerable to highly pathogenic influenza and other diseases with pandemic potential,[17] such that hundreds of thousands or millions could die worldwide.[18] The overall risk, therefore, can be assumed to be great. Further, due to the ability of viruses and bacteria to mutate or develop resistance to medications, pandemics may follow each other in rapid succession. Pandemic disease risk involving a highly pathogenic disease is as high every year as it was in 2009 (when the world was overdue for an influenza pandemic[19]) because a new strain will be responsible.[20]

(U) Depending on the severity of a pandemic disease that affects humans and how quickly it spreads, available critical infrastructure workforce numbers may be affected. All critical infrastructure sectors can be assumed to experience workforce reductions. However, risk for each sector will vary in terms of how much it depends on human resources to carry out sector responsibilities, how much of the sector must remain operational during times of emergency, and how long the sector can operate with less than optimal staffing. Eventually, absenteeism could affect the ability of all sectors to remain operational, compounding risk as services are disrupted and other sectors are affected as a result.

(U) Disease affects humans, animals, and plants. If pandemics occur for which medications and treatments are not available and the diseases spread very quickly,

---

new diseases, against which the human population has little or no immunity and for which the community has not yet had a chance to conduct sufficient research and develop medicines, treatments, etc. (e.g., Ebola); and (3) those caused by diseases to which populations have been exposed for many years that have developed mutations to get around population immunity, such that there are no or very few medicines currently available for those who have contracted these diseases (e.g., Extremely Drug Resistant Tuberculosis).

[n] (U) Healthcare research and development will continue to create new medicines and delivery methods. However, a number of issues will counter these medical advances. Growing national and global populations will increase the total number of people that could potentially be exposed to disease. Increasing urbanization could concentrate disease in larger groups and more confined spaces. The overuse and inappropriate distribution of antibiotics could create more antibiotic-resistant organisms for which new antibiotics will need to be produced (if possible). The same would hold true for the overuse and inappropriate distribution of antiviral medications. Faster and more transportation modes could continue to spread disease more quickly, resulting in what would appear to be the near-simultaneous appearance of disease in numerous places throughout the world.

[o] (U) The H1N1 influenza pandemic of 2009 is the most recent pandemic that resulted in larger than usual numbers of sick and dead.

resulting in large numbers of ill, it is possible that demands will exceed the ability of the agricultural, emergency management, medical, and public health communities to respond. Although the critical infrastructure sectors that are responsible for these efforts would be at greater risk due to this increased demand for services, if these sectors become incapable of rendering necessary disease and population health management services, risk will increase for all critical infrastructure sectors.

(U) Reduced workforces resulting from pandemic disease create the greatest risk for the Banking and Finance Sector (due to increased absenteeism and affected critical infrastructure upon which the sector is dependent),[21] Food and Agriculture Sector (if absenteeism is very high and so prolonged as to prevent sufficient food supply and distribution),[22] Healthcare and Public Health Sector (due to increased absenteeism and the increased costs to the healthcare system in general),[23] Information Technology Sector (due to operation and maintenance crew absenteeism),[24] Transportation Systems Sector (due to increased absenteeism),[25] and Water Sector (due to operator and support staff absenteeism, not direct human consumption).

(U) Increased demand for services to manage pandemic disease creates the greatest risk for the Food and Agriculture Sector (due to increased demand upon it to treat ill animals and plants), Healthcare and Public Health Sector (due to increased demand upon the healthcare system and public health community to treat ill humans),[26] followed by the Emergency Service Sector (if called upon to assist the Healthcare and Public Health Sector),[27] and Information Technology Sector (due to possible increased demand for services from locations other than work, if humans are most affected).[28] If demand for services is great enough, the Food and Agriculture Sector (in the case of pandemic animal disease) and the Healthcare and Public Health Sector (in the case of pandemic human disease) could cease to function entirely.

(U) Unintentionally Introduced Manmade Risks

(U) Unintentionally introduced manmade risks are those that are generated by humans, either accidentally or inadvertently. Accidental or inadvertent hazards may be the result of human error, poor calculations of risk, or negligence. Three unintentionally introduced manmade risks have been identified in the 2011 National Risk Profile as having potentially significant impact in the critical infrastructure context: industrial disaster risks, aging infrastructure risks, and economic instability risks.

(U) Industrial Disaster Risks

(U) Industrial disasters are commonly thought of as being the result of human and industrial process failures. However, industrial processes are run or designed by humans, so the common cause is ultimately human. Although it is understood that mechanical and other elements will wear out, break, etc. and that disasters may occur as a result, those large-scale or high impact industrial disasters that greatly affect the economy, the environment, and so on are of greatest concern. Aside from the potential for the catastrophic consequences associated with industrial disasters, the inability to do more with less and the inability to recognize unusual circumstances create the greatest risk for the critical infrastructure in the industrial context.

(U) The current state of the economy has resulted in higher levels of unemployment and the drive to increase profits by decreasing human and other resources costs throughout both the public and private sectors. As a result, fewer employees are available to operate, manage, maintain, repair, and otherwise enable the critical infrastructure to function. Additionally, increasing dependencies and interdependencies among critical infrastructure-related technologies often creates challenges for existing workforces, requiring expertise in a number of disciplines and skill areas. They are trying to do more with less.[p] Improved technology, increased technology, and more efficient business processes act to counter this problem and reduce risk in some cases. However, new technologies also can be more complex and create greater challenges to the workforce in being able to keep up with the skills needed and to cope with associated uncertainties. When sacrifices are made, risk to the critical infrastructure increases. Those activities perceived to be less important are postponed, broken parts of the physical critical infrastructure are replaced with cheaper and potentially lower quality substitutes, less experienced (and, presumably, less expensive) personnel are hired or retained, and so on.[q] Risk to the critical infrastructure grows as the ability to operate in this environment decreases. Moreover, the environmental conditions in which industrial operations are being carried out are becoming increasingly dangerous with highly uncertain potential impacts. Unabated, these situations can be expected to continue to increase risk and result in industrial accidents and disasters that vary only in magnitude.

[p] (U) For example, fatigue due to fewer personnel working longer hours has been a factor in many industrial disasters, including but not limited to the Deepwater Horizon oil spill, the Exxon Valdez oil spill, and Three-Mile Island. [*Severe Impact of Fatigue in the Workplace Examined*, EHS Today, http://ehstoday.com/news/ehs_imp_35340/, accessed June 25, 2011]

[q] (U) The Deepwater Horizon industrial disaster was said to be caused by many of these factors, including but not limited to postponed maintenance, decisions to sacrifice safety to save money, skipping procedures, and long deferred inspections. [Hilzenrath, D., *Hearings Focus on Possible Human Factors in BP Oil Spill,* The Washington Post, www.washingtonpost.com/wp-dyn/content/article/2010/07/22/AR2010072203444.html, accessed June 25, 2011]

(U) Many people are trained to do a particular job related to critical infrastructure. Having received that training and attained a certain level of expertise, they expect their worksite characteristics to remain mostly the same. However, changes do occur. Eventually these changes create unusual circumstances and increase the risk that critical infrastructure personnel could recognize if they had time, training, and previous experience with other unusual situations.[r] The inability to recognize, communicate,[s] and subsequently manage unusual circumstances contributes directly to critical infrastructure risk, but this risk can be reduced with additional training. Such training and education programs do exist and are provided by academia, the military, the government, and industry.[29] However, when funding is cut back, supposedly nonessential items (such as funding for training) are also often reduced.

(U) These human factors—the inability to do more with less and the inability to recognize, communicate, and manage unusual circumstances—have contributed to the occurrence of industrial disasters. If broadly defined, the risk for industrial disasters is present for all critical infrastructure sectors, and human factors discussed here are omnipresent throughout all of the sectors. However, when using a more common and strict definition of industry, the risk of industrial disaster is greatest for the Chemical Sector, Critical Manufacturing Sector, Defense Industrial Base Sector, Energy Sector, Food and Agriculture Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, and Water Sector because they are part of, directly reliant upon, or directly affected by industry.

(U) Aging Infrastructure Risks

(U) Critical infrastructure is aging.[30] Aging infrastructure[t] creates inefficiency when it renders parts of the critical infrastructure unusable. Deterioration also creates vulnerabilities.[31] These vulnerabilities may also be exploited by adversaries. Unusable, ineffectual, and deteriorating critical infrastructure, as well as the potential for exploitation of these vulnerabilities, increase risk.[32] While age undermines the capacity and resilience of critical infrastructure, age also may be exacerbated by initial problems in design (as a number of bridge failures have shown), lack of maintenance of facilities, or failure to adapt to unusual and unanticipated environments, all of which can reduce the theoretical or design life expectancies of critical infrastructure. The following aspects

[r] (U) For example, personnel on the Deepwater Horizon oil rig did not notice a dire warning, continuing their activities as if all operations were still normal. [Hilzenrath, D., *Hearings Focus on Possible Human Factors in BP Oil Spill,* The Washington Post, www.washingtonpost.com/wp-dyn/content/article/2010/07/22/AR2010072203444.html, accessed June 25, 2011]

[s] Communication is a key factor that shapes the ability of the workforce at all levels of management to prepare for, respond to, recover from, and mitigate industrial disasters. This has been brought out as a critical factor in many industrial disasters. It will require additional training at the very least and in some cases a change in culture.

[t] (U) Aging infrastructure is defined as infrastructure that over time has grown weaker, due to broke or worn out materials, components, or elements.

of aging infrastructure contribute the most to this risk: inadvertent introduction of flaws, reduced inspection and maintenance workforce, and insufficient investment.

(U) Mechanisms, procedures, and standards are put in place to ensure that the critical infrastructure is built to meet high functional standards. However, flaws are sometimes introduced inadvertently and not noticed until they are stressed over the course of time and reveal their associated vulnerabilities.[33] These flaws can be due to human error or to the introduction of counterfeit materials into the supply chain, which are subsequently and unknowingly used[u] to create physical and other critical infrastructure that then becomes inherently flawed, increasing risk.[34] Flaws in new and preexisting critical infrastructure could reveal themselves right away, but it is more likely that they will only become obvious when the critical infrastructure loses functionality or breaks over time. This risk has placed the critical infrastructure at greater risk than ever before.[35]

(U) Inspection procedures[v] should identify faulty mechanisms in complex machinery and other critical infrastructure elements that have ceased to function over time.[36] However, the inspection workforce that is charged with finding such faulty and broken mechanisms is itself aging, retiring, or facing reductions due to lack of funding for salaries.[37] Fewer personnel means fewer inspections and fewer opportunities to find flaws, faults, and other vulnerabilities in the critical infrastructure—flaws that are expected to contribute more to risk as the critical infrastructure ages.[38] As a result, risk is expected to increase until new personnel are hired to replace those who are departing and new funding is provided to enable them to not only identify but also rectify these problems. An additional consideration is that of personnel surety. It is essential that in the effort to replenish critical infrastructure ranks, the inspection workforce not be infiltrated by those who would seek to do the Nation harm, purposely covering faults and failures and increasing critical infrastructure risk further.

(U) Investments in various aspects of the critical infrastructure have decreased over the past 20 years,[39] and percentages of budgetary spending on the critical infrastructure have decreased over the past 50 years.[40] Insufficient investment extends beyond that of investing in personnel who inspect, run, and manage critical infrastructure. Funds are also needed for replacement parts,[w] patches, upgrades, and maintenance, as well as security against terrorism and natural hazards. Although it is obvious that critical infrastructure in all sectors is aging, increasing vulnerabilities and overall risk, it is not as widely understood exactly when investments need to be made to counteract this aging.

[u] (U) Inadequate inspection regimes and supply chain security—in the country that exports such counterfeit steel products and in the country that imports it—can leave builders incorrectly assuming that the materials they are using are sound.
[v] Unfortunately, some inspection guidelines miss key problem areas. For example, scouring of the bridge footings that led to the failure of the Schoharie Bridge in New York State went unnoticed, since inspection guidelines did not include subsurface inspection.
[w] (U) For example, for want of additional parts even after renovation, the Charles Berry Bascule drawbridge in Lorain, Ohio, was taken out of service and remained that way for months. [Kroll, J, *Lorain's Bascule Bridge Opens Today After Long Delay,* The Plain Dealer, blog.cleveland.com/metro/2008/11/lorains_bascule_bridge_opens_t.html, accessed April 26, 2011]

Made too early, such investments are a waste of money. Made too late, decisionmakers risk lives and property. Tradeoffs are particularly difficult to judge when insufficient data are available to determine exactly when something may break or malfunction and when insufficient funds exist to take action, regardless of the state of the critical infrastructure.

(U) Despite the best of intentions and recognition that funding should be provided, these investments are not expected to increase sufficiently[41] while the U.S. economy remains weak and while lawmakers continue to hope that the various critical infrastructure sectors will continue to function well enough until new and sufficient funding becomes available to make needed improvements. All of this may fall within what the Nation's leaders and citizenry consider their tolerance for inconvenience in the name of saving money. However, tolerance is much lower for loss of lives and property when critical infrastructure malfunctions. It is expected that aging infrastructure will continue to result in occasional industrial disasters. If greater investments are not made to counteract the effects of this aging, the rate of these disasters occurring could stay the same or increase. This will increase critical infrastructure risk as well as risk in other areas, including the economy, potentially causing the United States to fall behind other countries and regions economically, particularly China and Europe.[42]

(U) Aging will affect all critical infrastructure sectors. Attempts to counteract the ill effects will vary by critical infrastructure type and associated funding.

(U) Economic Instability Risks

(U) An unstable economy is characterized by a reduced government spending, high unemployment, inflation, and pronounced business cycles that also reduce private sector spending. Lack of public and private sector spending and unemployment contribute most to risk for the critical infrastructure, making it less reliable, safe, and secure.

(U) A certain amount of public funding and private sector spending[43] are required to maintain minimum critical infrastructure functionality. The further below that level funding falls, the greater the potential for critical infrastructure deterioration and reductions in personnel, and the more critical infrastructure risk increases. Government spending is not guaranteed in this age of massive cutbacks. Those parts of the critical infrastructure that are owned and operated more by the private (than public) sector could theoretically fare better than those that are more governmental. However, the private sector may not have the money available to invest nor the desire to invest what it possesses when the economy is unstable. Physical failure is possible and easy to envision, but failure may also include lack of service to and negative effects upon other types of critical infrastructure.

(U) Lack of public funding and private sector spending also result in decreased employment throughout the public and private sectors, including the critical infrastructure. Critical infrastructure employees are not just those that are responsible for mission execution (such as police, firefighters, and private security) and the operators of the critical infrastructure. They are also part of the team (including inspectors and builders) that ensures all critical infrastructure sectors function. All of these employee losses could increase risk to the critical infrastructure. Although greater job security characterized governmental and government-critical private sector jobs previously, it has become necessary to address the National deficit while also trying to stabilize the economy. Jobs associated with the critical infrastructure are essential to ensuring the public health, safety, and security of the Nation, but other jobs are also considered vital (e.g., defense-related jobs), and as a result, grants and other funding for critical infrastructure positions may not be top priority.[x] However, as with funding, there is a minimal level of staffing necessary to keep all critical infrastructure sectors functioning. Remaining staff may be able to take on additional responsibilities for a certain period of time, but eventually, people burn out, retire, or leave for more lucrative and less stressful positions.

(U) Those sectors that that are considered vital parts of the national security apparatus (such as the Defense Industrial Base Sector, Government Facilities Sector, and parts of the Transportation Systems Sector) may fare better, but an unstable economy could increase risk for all critical infrastructure sectors.

(U) Intentionally Introduced Manmade Risks

(U) Intentionally introduced manmade risks are created by those who deliberately choose to harm others for gain. Three intentionally introduced manmade risks have been identified in the 2011 National Risk Profile as having potentially significant impact in the critical infrastructure context: terrorism risks, border security risks, and cyber disruption risks.

(U) Terrorism Risks

(U//FOUO) The United States continues to be at risk from acts of terrorism[y] due to the persistent and evolving terrorist threat from a number of violent jihadist groups that are aligned ideologically with, but not necessarily directed by, al-Qa'ida, increasing risk to the critical infrastructure and the Nation. Public statements from groups sympathetic to

[x] For example, cuts in homeland security grants have resulted in police, firefighting, emergency services, and other reductions.

[y] (U) Terrorism is defined in the Code of Federal Regulations as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." [28 C.F.R. Section 0.85]

al-Qa'Ida indicate that the intent to strike the United States will continue.[44] These groups continue to be driven by their undiminished intent to attack the United States and to adapt and improve their capabilities.[45] The death of Usama bin Ladin on May 1, 2011 is unlikely to provoke core al-Qa'ida to attack in the near-term. However, the death of bin Laden may cause al-Qa'ida's affiliates and allies to accelerate their own existing plots.

(U//FOUO) Despite bin Ladin's death, it is expected that al-Qa'ida and its affiliates will continue to enhance their capabilities to attack through greater cooperation with regional terrorist groups. Historically, al-Qa'ida has focused on prominent political, economic, and critical infrastructure targets with the intent to produce mass casualties, visually dramatic destruction, significant economic aftershocks, and fear among the population. The group is innovative in creating new capabilities and overcoming security obstacles.[46]

(U//FOUO) The evolving and dynamic terrorist threat and the ever-increasing resilience of al-Qa'ida and other like-minded terrorist organizations also pose a significant threat to the Nation's critical infrastructure. Overall critical infrastructure risk is further amplified due to challenges in detecting terrorist plots underway. The current trend of tactics which use individuals or small groups that can act quickly and independently or with only tenuous ties to foreign handlers makes detection difficult. Operatives are assumed to be in the country and could attack with little or no warning. Attempted attacks and plots in the United States progressed to an advanced stage largely because these groups were able to use operatives that had easy access to and were familiar with the United States. Recent events also suggest that terrorists are seeking to conduct smaller, more achievable attacks against easily accessible targets.

(U//FOUO) These trends do not preclude the possibility of a large-scale attack, which also remains an important objective for al-Qa'ida. For example, as of February 2010, al-Qa'ida had identified Chicago, Los Angeles, New York City, and Washington, D.C. as important cities where large-scale attacks should occur. Al-Qa'ida, its affiliates, and its allies over the last two years have targeted large population centers in the United States with emphasis on conducting attacks intended to inflict mass casualties[47] and cause significant economic and psychological harm.[48] Mass gatherings, particularly those that occur during the summer months, are also expected to be attractive targets.[49] Rather, these trends reveal a belief that smaller-scale operations are more likely to succeed because they use fewer conspirators and more autonomous operatives, making it more difficult to identify and apprehend the plotters. This evolving threat has been highlighted by a number of recent domestic events, including the October 2010 cargo plot, the Times Square bombing attempt, the Fort Hood attack, and the December 2009 airline bomb plot.

(U//FOUO) The increasing prevalence and role of Westerners (including U.S. citizens) in al-Qa'ida and associated groups, either as leaders or operatives, gives these groups knowledge of Western culture and security practices that they would have found much more difficult to attain otherwise. U.S. persons who hold leadership positions in al-Qa'ida and associated groups have also called publicly on Western individuals to wage jihad by conducting attacks locally.

(U) Secretary Napolitano has stated that "…We face a threat environment where violent extremism is not defined or contained by international borders."[50] The threat of homegrown violent extremism[51] is also expected to grow,[52] increasing risks to the critical infrastructure sectors extremists choose to target. U.S. adversaries have recruited U.S. citizens and other persons residing within the Nation and its territories for decades, with more recent efforts dedicated to attempting to execute acts of terrorism.[53]

(U//FOUO) The use of explosives also continues to be a preferred tactic in terrorist attacks around the globe. IEDs can be combined with suicide tactics for delivery against a wide array of targets, contributing significantly to risk to the critical infrastructure. Explosive devices may be hand carried or vehicle borne, used as the primary attack method or as a key element of an armed assault against critical infrastructure. IEDs are often assembled *in situ* using homemade explosives which are manufactured with readily available consumer products. Terrorists are becoming more innovative in developing and using IEDs, often making them with homemade explosives (HMEs) in attacks against the United States. As the December 25, 2009 attempted bombing of Northwest Airlines Flight 253 by alleged perpetrator Umar Farouk Abdulmutallab demonstrated, international terrorists continue to develop and try to use new, innovative IEDs. In the case of Abdulmutallab, the device was composed of non-metallic components and concealed in his underwear in a deliberate attempt to evade common screening measures.[54] *Inspire* magazine, produced by Al-Qa'ida in the Arabian Peninsula (AQAP), contained a description of the device used in the October 2010 cargo plot and how AQAP avoided detection of the explosive-laden packages by metal detectors, sniffers, x-ray machines, and human inspection.[55] HMEs also were part of the failed plot by Najibullah Zazi to attack the New York City subway system after purchasing commercially available hydrogen peroxide beauty products for use in IEDs.
(U//FOUO) Every sector is potentially at risk for terrorism. Decentralization of terrorist groups increases risk throughout the Nation and its critical infrastructure. However, some sectors are at greater critical infrastructure risk due to expressed interest on the part of terrorists, larger potential consequences, and/or lower perceived security postures. The Commercial Facilities Sector, Government Facilities Sector, Banking and Finance Sector, and Transportation Systems Sector face greatest risk due to their

public accessibility, the high density of people in enclosed areas, and the potential for psychological impacts beyond an initial attack. The Chemical Sector, Dams Sector, Food and Agriculture Sector, and Water Sector are at greater risk due to the potential for large consequences. The Commercial Facilities Sector and Transportation Systems Sector are at greatest risk due to their vulnerability to small-scale operations. Although the use of IEDs contributes to risk for all critical infrastructure sectors, recent plots and events indicate that the Postal and Shipping Sector and Transportation Systems Sector continue to be at particular risk. Economically important critical infrastructure in the United States also remains a possible target.[z]

(U) Border Security Risks

(U) Threats and vulnerabilities at any part of the border create risk for the critical infrastructure.[aa] The greatest border security[56] risks to critical infrastructure are caused by lack of personnel security, importation and use of counterfeit materials, and exploitation of vulnerabilities where critical infrastructure is located at the border.

(U) Criminal aliens and terrorists taking advantage of poor personnel security practices to destroy or otherwise eliminate the use of critical infrastructure are of concern.[57] The risk created by criminals and terrorists obtaining positions illegally (e.g., by presenting false documents[58] and obtaining Social Security numbers illegally[59]) is high when organizations do not adhere to the law[60] by not checking backgrounds, not ensuring they have the resources to effectively confirm the identity of new employees, or not believing that criminals or terrorists will ever try to infiltrate their ranks and seek to harm or destroy the critical infrastructure. This risk is also high when law enforcement does not have the resources to ensure that employers are adhering to legal employment requirements and to investigate cases where they suspect that the law has been broken in this regard.[61]

(U) The movement of counterfeits across the border also increases risk to the critical infrastructure. Counterfeit materials have been introduced into the global supply chain and as a result, they have been imported into the United States. Some of these materials, such as counterfeit steel components,[62] could be unknowingly used to fix or build critical infrastructure[63] if not tested in advance. Counterfeit bearings,[64] circuit breakers,[65] and critical technology components[66] have been imported into the United States (intentionally by the exporters and intentionally or unintentionally by the importers) and could also be used to fix or build critical infrastructure.[67] The risk of exacerbating preexisting lack of functionality within all critical infrastructure sectors, as

[z] (U//FOUO) AQAP publicly called for attacks against U.S. financial and commercial entities in 2010 and 2011 issues of its magazine *Inspire*.

[aa] (U) Critical infrastructure assets occupy space on and in land, sea, and air, as well as cyberspace.

well as creating problems that may only be detected months or years after parts of the critical infrastructure have been created and put in place, increases as lack of inspection, insufficient enforcement of export/import laws, and inadequate enforcement of counterfeiting laws increase.

(U) Risks to critical infrastructure found at the border increase as vulnerabilities are exploited at the border. Bulk cash smuggling,[68] poorly controlled transportation of chemicals,[69] Global Positioning System (GPS) jamming,[70] counterfeit materials,[71] power coming from Canada with uncertain reliability,[72] pests and disease,[73] and conflicts regarding water flowing across the border to Mexico[74] are all examples of problems that reveal or take advantage of vulnerabilities at the border. Reliance on interdiction and after-the-fact response requires more resources than can be made fully and quickly available whenever borders are breached. For those border areas that have become so insecure (due to lawlessness on the Mexican side of the border) that funding must be increased for security, that funding may be diverted from other areas, such as the critical infrastructure. The longer the border areas remain uncontrolled, the less secure the United States and the greater the risk to the critical infrastructure.

(U) Border security risks could potentially affect all critical infrastructure sectors. Risk from lack of personnel security is greater for the Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Food and Agriculture Sector, Healthcare and Public Health Sector, Information Technology Sector, Postal and Shipping Sector, and Transportation Systems Sector (as these sectors have often been found to employ—knowingly and unknowingly—improperly documented persons). Risk due to illegal and inadvertent importation and incorporation of counterfeit materials for use by the critical infrastructure is least for the Nuclear Reactors, Materials, and Waste Sector (owing to the strict controls and inspection mechanisms used by the sector to protect against this threat and reduce this risk). Risk due to the exploitation of border vulnerability is greatest for the Transportation Systems Sector, but the Banking and Finance Sector, Chemical Sector, Communications Sector, Critical Manufacturing Sector, Energy Sector, Food and Agriculture Sector, Healthcare and Public Health Sector, Information Technology Sector, Postal and Shipping Sector, and Water Sector are also at risk (as these sectors conduct operations or send goods and services across the border).

(U) Cyber Disruption Risks

(U) The United States has become a society dependent on network-based technology and electronic processes and communication, and the disruption of any of these is considered a cyber disruption. All critical infrastructure sectors are dependent on cyber systems to some extent. As a result of our societal dependence and the cross-cutting

nature of cyber disruption risks, the critical infrastructure community faces new challenges regarding cyber disruption. The greatest cyber disruption risks are due to attacks on the cyber infrastructure[bb] and continuous adaptation of the threat.

(U) Intentional, unintentional, physical, logical, or blended attacks create cyber disruption.[cc] Although cyber disruption could be generated by terrorists, this does not have to be the case. Because cyber infrastructure is interdependent and interconnected, the opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside an organization are vast, contributing to critical infrastructure risk. The sheer number and sophistication of disruptive cyber attacks demonstrate that the cyber infrastructure of the United States is increasingly vulnerable[75] and that associated risks are increasing. Potential adversaries[dd] perpetrating these attacks vary according to type of attack and target. Increased risk to public utilities and other critical infrastructure (regarding the impact upon time-sensitive operations that underpin their functions that may be disrupted or manipulated to cause accidents or disasters) is of particular concern. The risk of cyber disruption of critical infrastructure and the number and skill of enemies to execute such attacks are expected to increase.[76] It is also likely that cyber attacks will be used as part of a diversified strategy to attack the homeland.[77]

(U) The cyber threat[78] adapts to cybersecurity practices. The critical infrastructure risk from cyber disruption is expected to remain the same or increase with such adaptations.[79] Risk to the critical infrastructure also is increasing with the rising number of zero-day vulnerabilities (flaws in software code discovered before fixes or patches are available), the steady increase in the number of individuals capable of exploiting these vulnerabilities, and the near-static average time for developing patches.[ee] Individual cybersecurity habits lag behind both the threat and the tools available to protect critical infrastructure and information systems,[80] thereby also increasing critical infrastructure risk.[81]

[bb] (U) Cyber infrastructure includes electronic information and communications systems and the information in those systems. The three broad categories of cyber critical infrastructure are Business Systems, Control Systems, and Access Control and Other Specialty systems. [Analysis from the Department of Homeland Security, National Cyber Security Division, Critical Infrastructure Protection Cyber Security (CIP CS) Program, April 2011.] Information and communications systems are composed of hardware and software that process, store, and communicate information and data. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. [Department of Homeland Security, *National Infrastructure Protection Plan 2009*, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed May 13, 2011]

[cc] (U) Blended attacks are when conventional physical attacks are accompanied by a logical attack to disorient the target, similar to electronic warfare. [Organization for Economic Cooperation and Development. *Reducing Systemic Cybersecurity Risk*, January 2011.]

[dd] (U) Cyber threat actors include large-scale criminals, hactivists, recreational hackers, nation-states, and terrorists.

[ee] (U) According to the SANS Institute, "zero-day exploits in client-side applications [are] one of the most significant threats to your network, and requires that you put in place additional information security measures and controls to complement your vulnerability assessment and remediation activities." The Institutes website includes over 25 vulnerabilities of medium or high severity that were identified one year ago or more, yet still do not have a fix or patch in place. [The SysAdmin, Audit, Network, Security (SANS) Institute, *The Top Cyber Security Risks*, September 2009, http://www.sans.org/top-cyber-security-risks/summary.php, accessed June, 27, 2010]

(U) Widespread and otherwise nationally significant cyber disruption potentially places all critical infrastructure sectors at risk. Those critical infrastructure sectors that are vulnerable to cyber and other attacks will be at the greatest risk for cyber disruption, and this risk will increase as the Nation's information technology level advances.[82] The risks to the Banking and Finance Sector, Communications Sector, Energy Sector, and Transportation Systems Sector will be greater to begin with due to their current high-level utilization of cyber critical infrastructure to support their capabilities and functions.[83]

(U) The following cyber threats are expected to increase the risk of cyber disruption for certain critical infrastructure sectors more than others: Stuxnet[ff] deployment (expected to affect the Critical Manufacturing Sector, Dams Sector, Healthcare and Public Health Sector, Nuclear Reactors, Materials, and Waste Sector, Postal and Shipping Sector, and Transportation Systems Sector because the Stuxnet worm attacks the control systems these sectors depend on), computer-aided dispatch[84] failure (expected to affect the Emergency Services Sector, Postal and Shipping Sector, and Transportation Systems Sector because these sectors are dependent upon mobile data terminals), GPS jamming[85] (expected to affect the Communications Sector, Emergency Services Sector, Food and Agriculture Sector, Postal and Shipping Sector, and Transportation Systems Sector because of their dependence on this technology), and short message service mass mobile alert exploitation[86] (expected to affect the Commercial Facilities Sector, Communications Sector, Emergency Services Sector, Government Facilities Sector, and Transportation Systems Sector because of their dependence on this technology). The complex interconnections among critical infrastructure sectors, as well as common dependence on electronic information and communication systems, make the cyber role in critical infrastructure extremely important. This complexity means that cyber attacks directed at a single sector may affect others—potentially resulting in cascading failures. More specifically, cyber attacks directed at the Information Technology Sector, Communications Sector, Energy Sector, and Banking and Finance Sector could affect these sectors as well as other critical infrastructure sectors with which these sectors are interdependent.

[ff] (U) Stuxnet is a worm that attacks control systems, potentially taking control of control systems or stealing code and design projects.

(U) Sector Risks

(U) The critical infrastructure sectors experience naturally occurring and manmade risks related to the unique characteristics of each sector, as well as the cross-cutting risks described above. Additionally, sectors are dependent and interdependent upon one another to varying extents. Risks that have potentially significant impact in the critical infrastructure context are presented in the 2011 National Risk Profile according to each sector. There may be cases where the national risks may not be as great to a particular sector but still create cross-cutting risk. National risks that could potentially affect particular sectors will only be discussed in this section if from the perspective of the sector those cross-cutting risks are considered amongst the most significant.

(U) Risks to the Banking and Finance Sector

(U) The Banking and Finance Sector accounts for more than eight percent of the U.S. annual gross domestic product and is the backbone for the world's economy.[87] The sector is primarily owned and operated by the private sector, and its institutions are extensively regulated.[88] The sector's products and services include deposit, consumer credit, and payment systems; credit and liquidity products; investment products; and risk-transfer products (including insurance).[89] The sector faces current and ongoing risks due to cyber attacks, insider threats, pandemic disease, and large-scale physical attacks.

(U) The threat of cyber attacks poses the most significant risk to the Banking and Finance Sector.[90] Terrorists, transnational criminals, and foreign intelligence services are becoming aware of and are using computer viruses, Trojan horses, worms, logic bombs, eavesdropping sniffers, and other tools that can destroy, intercept, degrade the integrity of, or deny access to data.[91] Other potential cyber threats to the sector include confidentiality and identity breaches, emerging technology, professionalization of cyber criminals, and continued globalization of the sector.[92] The consequences of a successful widespread cyber attack on the Banking and Finance Sector could include erosion of public confidence in financial institutions, denial of business and individual access to funds, loss of funds, loss of financial information integrity, and inhibition of securities trading.[93]

(U) The insider threat also presents ongoing risks to the sector. Such attacks could come from individuals or groups with malicious intent, including disgruntled employees, organized crime, or even those with unwitting intent. The disgruntled insider is a significant threat since these individuals often have knowledge that allows them to gain

unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions.[94] As financial institutions eliminate redundant operations and reduce personnel costs, these reductions can lead to vengeful acts by departing employees, as well as by dissatisfied employees among the remaining staff.[95] Insider attacks can also happen by unwitting employees or third parties, who unintentionally damage, destroy, or steal data.[96]

(U) Physical events caused by natural hazards or other large-scale terrorist attacks could cause significant economic losses to the sector and to the Nation.[97] Regulators responsible for safety and soundness issue guidelines and specific regulations requiring redundancy and security in physical and financial systems[98] and have long required banking institutions to consider addressing operating (security) risks in their contingency plans.[99] While these measures were effective and the sector saw little impact on September 11, 2001,[100] and during the Northeast Blackout of 2003[101] and Hurricane Katrina,[102] risk to the sector is ongoing as the Nation continues to experience a high frequency of natural hazards and as the sector continues to face the possibility of a large-scale terrorist attack.

(U) The Banking and Finance Sector is critically dependent upon the Energy Sector, Information Technology Sector, Transportation Systems Sector, and Communications Sector.[103] The sector also relies on an extensive and complex supply chain,[104] often reaching to providers outside the United States, including a significant number of third-party providers.[105] The sector is interdependent with the Commercial Facilities Sector as that Sector it is highly reliant on the Banking and Finance Sector for financial transactions associated with cash, checks, and credit cards,[106] and the Banking and Finance Sector's administrative offices are often located in Commercial Facilities Sector buildings.[107]

(U) Risks to the Chemical Sector

(U) The Chemical Sector is an integral component of the U.S. economy, employing nearly one million people and earning revenues between $600 and $700 billion per year.[108] The Chemical Sector is composed of five main segments, based on the types of end products: basic, specialty, and agricultural chemicals; pharmaceuticals; and consumer products. The sector faces current and increasing risks due to the vulnerability of network-based control systems, insider threats, and natural disasters and accidents.

(U) The Chemical Sector is and is expected to remain at risk from the threat of malicious actors physically or remotely manipulating network-based systems designed to control chemical manufacturing processes or process safety systems. Should a

malicious actor succeed in overriding control system security, the result could be catastrophic.[109] The physical disruption inflicted upon industrial assets in 2010 by the Stuxnet worm is evidence that control systems are vulnerable to increasingly destructive attacks and that U.S. critical infrastructure may face cyber attacks of increasing sophistication.[110]

(U) While a facility can increase its physical security measures substantially, the Chemical Sector will continue to face risk from insiders with access who choose to intentionally cause harm.[111] Factors that may hinder management of the insider threat include greater competition and less cooperation among owners and operators within the sector and relatively low cooperation between owners and operators and their workforces.[112]

(U) Natural disasters and accidents pose an ongoing risk of exposing the environment and the population to chemicals. Accidents such as the 2001 AZF chemical fertilizer plant blast, an ammonium nitrate explosion that resulted in 29 deaths and 2,500 injured in Toulouse, France, demonstrate the significant potential consequences of incidents involving harmful chemicals.[113] U.S. facilities are also at risk, as seen in the 1989 explosion at the Houston Chemical Complex, which killed 23 employees, injured 130 others, and caused nearly three-quarters of a billion dollars in damages.[114] Much of the U.S. petrochemical industry also is located along the Gulf Coast and is, therefore, vulnerable to hurricanes.

(U) The Chemical Sector is critically dependent upon the Transportation Systems Sector, which facilitates the transfer of precursor chemicals within the industry, and the Energy Sector, which provides power for the energy-intensive Chemical Sector's industrial processes. The Nuclear Reactors, Materials, and Waste Sector, Critical Manufacturing Sector, Water Sector, Agriculture and Food Sector, and Healthcare and Public Health Sector are all critically dependent upon the Chemical Sector, with the Food and Agriculture Sector and the Healthcare and Public Health Sector representing an especially large number of mission-critical capabilities.[115]

(U) Risks to the Commercial Facilities Sector

(U) Widely diverse in scope and function, the Commercial Facilities Sector is composed of eight subsectors: public assembly, sports leagues, gaming, lodging, outdoor events, entertainment and media, real estate, and retail.[116] The sector primarily comprises privately owned facilities that are open to public access.[gg] The sector faces ongoing and

[gg] (U) Public assembly is typified by arenas, stadiums, aquariums, zoos, museums, and convention centers; sports leagues by professional sports leagues and federations; gaming by casinos; lodging by hotels, motels, and conference centers; outdoor events by theme and amusement parks, fairs, campgrounds, and parades; entertainment and media by motion picture studios and

increasing risks from three threats: bombing, active shooters, and terrorist attacks using CBRN weapons or agents.

(U) Commercial facilities are at increased risk due to the threat of bombings that have the potential for creating mass casualties, that are symbolically important (as at major sporting events),[117] in which the adversary had expressed interest,[118] and that could follow the precedence of previous attacks. U.S. sector facilities have been targeted in the past, including the World Trade Center in 1993,[119] the Atlanta Olympic Park in 1996,[120] and the attempted Times Square attack in 2010,[121] and al-Qa'ida will likely continue to target soft, economic targets.[122] The sector's principle of open public access limits the use of highly visible security barriers, which increases vulnerability to all attacks[123] and thereby increases risk for the sector. Commercial targets are also frequently attacked overseas, as seen in the bombings of hotels in Jakarta,[124] Islamabad,[125] and Mumbai,[126] due to the high visibility of attacks, limited security measures, and large casualty numbers.[127]

(U) The sector is also at risk from the active shooter threat.[hh] Worldwide, firearm attacks in general have spiked dramatically,[128] and al-Qa'ida appears to be transitioning to less spectacular, smaller scale attacks including firearms.[129] While active shooter attacks may produce fewer casualties, they do not require the resources and planning needed for more sophisticated, innovative attacks.[130] As with bombings, the sector's open public access and high density of individuals leave it vulnerable to active shooters. This vulnerability can be seen in the 18 criminal shootings that occurred in U.S. retail locations between 2004 and 2008.[131] As a result, these vulnerabilities increase risk to the sector.

(U) The sector is also at increased risk from the threat of terrorists using CBRN weapons or agents. Some terror groups remain interested in acquiring CBRN materials and threaten to use them.[132] Radiological attacks could be executed indoors, such as disseminating irradiated powders through the ventilation system of a large building or sports arena[133] or hiding a radiation source in a location, such as a theater, where large numbers of people could be exposed.[134] Outdoor facilities, such as public assemblies or sporting events, are also at risk. Al-Qa'ida has expressed interest in obtaining crop dusters, which could be used to disseminate aerosolized CBRN agents over large areas and gatherings.[135]

---

broadcast media; real estate by office and apartment buildings, condominiums, mixed-use facilities, and self-storage; and retail by retail centers and districts and shopping malls. [Department of Homeland Security, *Commercial Facilities Sector: Critical Infrastructure and Key Resources*, accessed at www.dhs.gov/files/programs/gc_1189101907729.shtm on May 13, 2011]

[hh] (U) DHS defines an active shooter as "an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms." [DHS, "Active Shooter: How to Respond," October 2008, assessed at www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf on June 14, 2011]

(U) The Commercial Facilities Sector is critically dependent on the Agriculture and Food Sector, Banking and Finance Sector, Communications Sector, Critical Manufacturing Sector, Emergency Services Sector, Energy Sector, Healthcare and Public Health Sector, Information Technology Sector, Postal and Shipping Sector, Transportation Systems Sector, and Water Sector. The Commercial Facilities Sector and the Banking and Finance Sector, Critical Manufacturing Sector, and Emergency Services Sector are interdependent. [136]

(U) Risks to the Communications Sector

(U) The Communications Sector is a diverse, competitive, and interconnected industry that uses terrestrial, satellite, and wireless transmission systems to transmit information. While the loss of a single communications facility or key node is unlikely to significantly impact the Nation's communications systems, the loss could have cascading impacts on other critical infrastructure.[137] The sector is exposed to risk from cyber and insider threats and vulnerability to space weather and loss of power.

(U) The Communications Sector is at risk from cyber and insider threats. Single physical incidents are unlikely to disrupt the sector because the communications industry applies the principle of diversity, employing various primary and alternative routing and systems, and the principle of redundancy, using backup or multiple capabilities to sustain business operations. Cyber risks present unique challenges, however, because exploits of a vulnerability introduced halfway around the world can begin affecting critical U.S. communications components in a matter of minutes.[138] Malicious insiders also pose one of many human risks, which can impact organizations' data, networks, and components, as well as create financial losses.[139]

(U) In addition to adversary threats, the sector is exposed to naturally occurring risks from space weather, which could directly degrade communications satellites and disrupt GPS functionality—interfering with GPS satellites and their signals.[140] As the Communications Sector infrastructure evolves toward an all-digital environment, accurate timing and synchronization functions are becoming more critical, increasing the commercial use of GPS for communications applications. Short-term loss or disruption of GPS will have minimal impacts, but medium- to long-term loss will degrade services, including wireless, satellite, cable, and broadcast networks.[141]

(U) The Communications Sector is critically dependent upon two sectors: the Energy Sector, which provides power to run cellular towers, central offices, and other critical communications facilities, and the Information Technology Sector, which provides critical control systems and services, physical architecture, and Internet

infrastructure.[142] The Communications Sector is interdependent with the Government Facilities Sector, Transportation Systems Sector, and Water Sector.[143]

(U) Risks to the Critical Manufacturing Sector

(U) The Critical Manufacturing Sector is composed of manufacturing assets in the primary metals, machinery, electrical equipment, and transportation equipment.[144] The sector is crucial to the economic prosperity and continuity of the United States.[145] The sector strives to protect its facilities and supply chain without compromising accessibility, profitability, and the free flow of commerce. The Critical Manufacturing Sector faces current and increasing risks due to supply chain vulnerability, cyber intrusion, and malicious insider threats.

(U) Critical infrastructure risk to the Critical Manufacturing Sector is increasing due to heightened supply chain vulnerability. This vulnerability is driven by trends toward increasing the efficiency of supply chains,[146] as well as globalization, decentralized production, and the reduced number of materials suppliers.[147,148] Supply chain disruption at key inbound transportation nodes is of particular concern because incidents at nodes such as domestic ports are likely[149] and because of the potential for large-scale consequences to the many industries that rely on the importation of materials and products.[150] Lean inventory and just-in-time practices, as well as greater distances to deliver products, have made the Critical Manufacturing Sector more sensitive to transportation disruptions and fuel costs.[151]

(U) The threat within the Critical Manufacturing Sector of cyber intrusion into sector industrial control systems and supervisory control and data acquisition systems poses a growing risk. Critical manufacturing supply chain systems are more vulnerable because of an increased reliance on advanced information technology systems.[152] Critical infrastructure owners and operators are slow to adopt security and risk mitigation measures for systems.[153] Attacks such as Stuxnet suggest that cyber attacks may originate more often from nation-states and target U.S. critical infrastructure, including the industrial assets found in the Critical Manufacturing Sector.[154]

(U) The malicious insider threat also poses risks to the Critical Manufacturing Sector. The sector's complex and increasingly information technology-dependent systems make the sector highly susceptible to exploitation by current and former industry employees and contractors with malicious intent and unique knowledge of, and access to, these systems.[155] Threats posed by malicious insiders may include sabotage, theft or diversion, or cyber attack against critical manufacturing facilities.[156]

(U) The Critical Manufacturing Sector is critically dependent on the Transportation Systems Sector, due to heavy reliance of manufacturing on the transportation modes that support the supply chain,[157] the Energy Sector, which provides power to manufacturing facilities and fuel to supply chain transportation modes, and the Chemical Sector, as a supplier.

(U) Risks to the Dams Sector

(U) The assets in the Dams Sector include dam projects, hydropower generation facilities, navigation locks, levees, mine tailings, and other water retention and flood control facilities.[158] These assets not only support critical services, but their failure, damage, or disruption could also lead to loss of life, massive property damage, and severe long-term consequences.[159] The Dams Sector faces current and increasing risks due to natural hazards, the use of explosives by adversaries, and aging infrastructure.

(U) Natural hazards present ongoing threats to the sector, creating persistent risk. For example, extreme flooding and severe storm surges can overwhelm the flood storage capacity of reservoirs and levee systems and lead to breaching or overtopping.[160] The consequences of extreme levee failure were seen in the aftermath of Hurricanes Katrina and Rita in 2005, which resulted in the deaths of more than 1,800 people and more than $200 billion in economic damages.[161] Earthquake ground motion may also lead to severe damage or failure, as evidenced by the failure of Fujinuma Dam in Japan following the Tohoku earthquake in March 2011.[162]

(U//FOUO) Determined adversaries with the necessary capabilities and resources could potentially achieve catastrophic failure and severely disrupt missions through the use of improvised explosive devices (IEDs),[163] increasing risk for the sector. Adversaries could bypass land-based security measures with water-borne IEDs and strike dams, locks, or levees.[164] Vehicle-borne IEDs (VBIEDs) could also reach the crest of dams, particularly those with public highways that allow full access to the dam.[165] An assault team could overpower security forces, seize a facility's control room, and detonate IEDs, as occurred in a July 2010 attack against a Russian hydropower station.[166] Dams Sector assets have experienced at least 20 kinetic attacks worldwide over the last decade,[167] and adversaries could exploit the inherent vulnerabilities of these public facilities. Critical infrastructure risk to the sector is increasing as the threat from malicious actors using IEDs grows.

(U) The aging of the Nation's dams, levees, and waterway navigation structures continues to create risk for the Dams Sector.[168] Dams, inland waterways, and levees are in increasingly poor condition owing to aging, deterioration, and lack of

maintenance.[169] At least 1,065 dams have already exceeded their design life, as have almost half of all federally owned navigation locks.[170] This vulnerability increases the risk to the Dams Sector as its infrastructure continues to age.

(U) The Dams Sector is critically interdependent with the Water Sector, regarding water supply services; the Energy Sector, regarding operation of locks and hydroelectric power; the Transportation Systems Sector, regarding river navigation; and the Government Facilities Sector.[171]

(U) Risks to the Defense Industrial Base Sector

(U) The Defense Industrial Base Sector includes those elements of the Department of Defense, the U.S Government, and the private sector worldwide industrial complex that maintain capabilities of performing research and development, design, production, delivery, and maintenance of military weapon systems, subsystems, components, or parts to meet military requirements.[172] The sector is an extraordinarily large, diverse, complex, and interdependent collection of assets, owners, and operators, composed of hundreds of thousands of worldwide government and private sector sites.[173] Due to the sector's sensitive work, as well as continuous adversarial threats,[174] the Defense Industrial Base Sector promotes security awareness, which helps mitigate its risk. However, the threats of cyber disruption and loss of supply chain integrity raise risk for the sector.

(U//FOUO) The cyber threat creates the most pressing and important risk for the sector.[175] The Defense Industrial Base Sector has become heavily dependent on cyber infrastructure, operating within an increasingly information-driven environment.[176] The sector's cyber infrastructure is vulnerable to denial-of-service attacks and malicious modification of information, along with more mundane, yet disruptive, events, like system malfunctions, power outages, and human error.[177] This combined with the occurrence of increasing cyber attacks across the critical infrastructure community[178] contributes greatly to the risk to the sector. Foreign entities are also expected to continue seeking to acquire access to sensitive and classified Defense Industrial Base information and technologies by expanding their cyber collection activities.[179]

(U//FOUO) Globalization has created dependencies and interdependencies in the Defense Industrial Base Sector production supply chain that represent potentially dangerous points of failure for the sector. For example, sector-related industries depend heavily on assets outside of their direct control, including the global supply chain.[180] Due in part to a lack of traceability from foreign producers,[181] the potential for loss of supply chain integrity increases risk for the sector. This is highlighted by the ongoing infiltration

of counterfeit electronics into the sector.[ii] Lack of supply chain integrity could lead to the introduction of counterfeit and substandard materials, components, and technology into military equipment, which could, in turn, lead to equipment failures and increasing risk in the field.[182]

(U) The Defense Industrial Base Sector is critically dependent on the Communications Sector, Energy Sector, Healthcare and Public Health Sector, Information Technology Sector, Transportation Systems Sector, and Water Sector. The Defense Industrial Base Sector, the Commercial Facilities Sector, and Critical Manufacturing Sector are interdependent.[183]

(U) Risks to the Emergency Services Sector

(U) The Emergency Services Sector is a system of response and recovery elements that forms the nation's first line of defense, prevention, and management of consequences from disasters and terrorist attacks.[184] The sector includes eight areas of the response and recovery process: emergency management, emergency medical services, fire, hazardous material, law enforcement, bomb squads, tactical operations/special weapons assault teams, and search and rescue.[185] The sector is at risk from vulnerabilities owing to the lack of standardized and common communications resources and the threat of terrorist attacks using hazardous materials and CBRN agents. Transportation systems need to be functional for emergency response and operations.

(U) Communications vulnerabilities create ongoing risk for the sector. Communications channels and equipment standards have improved dramatically in the last several years.[186] However, many jurisdictions still struggle to use standardized code when communicating, have difficulty obtaining bandwidth to transmit their communications, lack interoperable communications equipment, and do not share frequencies among the various member organizations of the sector (e.g., police and fire).[187] Inability to communicate creates greater risk for the sector and for those who depend on the sector for its emergency services.

(U) The threat of terrorist attacks poses significant risk to the Emergency Services Sector.[188] Fire, police, hazardous materials, and other emergency service units respond to both suspected terrorist events (e.g., mailed letters and packages containing white

[ii] (U) A 2010 Department of Commerce study revealed that 39 percent of companies and organizations surveyed encountered counterfeit electronics, and it identified an upward trend in detected incidents, rising from 3,868 incidents in 2005 to 9,356 in 2008. [U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics,* January 2010, www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf, accessed May 10, 2011]

powders that could contain anthrax[189]) and executed terrorist events (e.g., the bombing of the Oklahoma City Murrah Federal Building, the events of September 11, and the anthrax events of 2001). As a result, emergency services personnel are exposed to substances of unknown composition, for which their personal protective equipment may or may not provide adequate protection.[190] In addition, adversaries may target persons in positions of authority[191], as well as institutions that would be symbolic of functioning society.[192]

(U) The Emergency Services Sector is critically dependent upon the Communications Sector, Energy Sector, Information Technology Sector, and Transportation Systems Sector. The Emergency Services Sector, Critical Manufacturing Sector, Government Facilities Sector, Healthcare and Public Health Sector, and Water Sector are interdependent.

(U) Risks to the Energy Sector

(U) The Energy Sector consists of two subsectors: electricity and oil and natural gas. These subsectors include thousands of assets that are geographically dispersed and connected by systems and networks.[193] The sector is exposed to risk through cyber attacks, physical attacks, and natural hazards.

(U//FOUO) Ongoing vulnerability to cyber attacks contributes significantly to the sector's risk. Electric power assets are potentially vulnerable to cyber attacks because the electricity infrastructure is highly automated and controlled by utilities and regional grid operators, who rely on sophisticated energy management systems. For example, assets may be vulnerable if the electricity subsector's control system networks ~~are~~ are connected to the corporate business network, which, in turn, is connected to the Internet. These connections increase the network's vulnerability to direct cyber attacks that could potentially disrupt power and increase risk to the sector. Insider cyber threats, such as those initiated by current or former employees, also create risk to the electricity subsector.[194] These vulnerabilities are ~~exacerbated~~ addressed to varying degrees ~~by the inconsistent levels of cyber defenses~~ across the Energy Sector which ~~follows its own~~is a mix of voluntary and mandatory security standards that apply to electricity grid owners and operators.[195]

(U) The threat of physical attacks also contributes to risk for the sector, which has become a favorite target for adversaries overseas. Worldwide, terrorists have executed 2,523 attacks against energy infrastructure since 2004, leaving 1,852 dead and 4,653 wounded.[196] Moreover, successful strikes against individual sector assets can lead to nationwide impacts that also contribute to risk. An attack or naturally-occurring event in the United States could also produce such large-scale consequences.

(U//FOUO) Natural hazards pose a regular and persistent risk for the sector. Hurricanes are the most frequent disruptive natural hazards for the oil and natural gas subsector, often causing the preemptive shutdown of facilities in an area, even if the facilities themselves are not directly affected by the storm.[197] Hurricanes Ike and Gustav in 2008 impacted almost 65 million barrels of crude oil production and 400 billion cubic feet of natural gas supply.[198] An additional natural hazard is that of solar storms, especially as they affect the energy grid.

(U) The Energy Sector is critically dependent on the Banking and Finance Sector, Communications Sector, the Information Technology Sector, and Transportation Systems Sector. All critical infrastructure sectors depend on the Energy Sector for essential energy supplies.[199] The Energy Sector is interdependent with the Communications Sector, Government Facilities Sector, Information Technology Sector, Transportation Systems Sector, and Water Sector.

(U) Risks to the Food and Agriculture Sector

(U) The Food and Agriculture Sector is composed of complex production, processing, and delivery systems and encompasses upward of four million assets, including some two million farms; more than 900,000 restaurants; more than 100,000 food retail establishments; more than 166,000 registered domestic food manufacturing, processing, and holding facilities; and approximately 252,400 registered foreign facilities.[200,201] The open nature and global interconnectivity of the sector presents unique security challenges and leaves the sector vulnerable to a variety of threats. Direct attacks on the sector, such as the introduction of animal or plant disease or deliberate food contamination, could result in devastating animal, plant, or public health and economic consequences.[202] The sector faces ongoing and increasing risks due to food contamination, disease and pests, and severe weather.

(U) A primary risk driver for the Food and Agriculture Sector is the threat of food contamination, whether by accidental or intentional means. Contaminated food in the United States is estimated to be responsible for over 47.8 million illnesses, 127,839 hospitalizations, and 3,037 deaths, costing the Nation more than $14 billion a year in terms of medical care, lost productivity, chronic health problems, and deaths.[203,204,205,206] Violent extremists have indicated an interest in poisoning the food supply with biological and chemical agents, which could have great potential to cause costly economic losses in the supply chain for implicated foodstuffs, create public panic, and lead to a public health crisis with considerable mortality and morbidity.[207,208,209,210]

(U) The threat of disease and pests represents an additional key risk factor for the Food and Agriculture Sector. The accessibility of crops and animals on the farm and the

extensive international and interstate movement of animals and products increase the sector's vulnerability to acquire and rapidly spread disease. Modeling estimates and historical evidence demonstrate that a domestic outbreak of a foreign animal disease, such as foot-and-mouth disease, would cost the United States billions of dollars from the loss of livestock, production, and international trade.[211,212,213]

(U) Severe weather, including droughts, floods, and climate variability, also presents an important risk to the Food and Agriculture Sector and critically influences farm productivity.[214,215] Weather and climate characteristics such as temperature, precipitation, carbon dioxide, and water availability directly impact the health and well-being of plants and livestock, as well as pasture and rangeland production. The deleterious effects of severe weather coupled with global climate change are currently affecting U.S. water resources, agriculture, land resources, and biodiversity, and this trend is expected to continue.[216]

(U) The Food and Agriculture Sector is critically dependent upon the Water Sector; Chemical Sector; the Dams Sector; Government Facilities Sector; Energy Sector; Transportation Systems Sector, which interconnects critical system nodes; Commercial Facilities Sector, which includes food processing plants, warehouses, and retail outlets essential to processing and distributing food products; and Banking and Finance Sector, as considerable financial transactions are involved in the purchase, processing, storage, and selling of farm commodities.[217,218]

(U) Risks to the Government Facilities Sector

(U) The Government Facilities Sector is concerned primarily with ensuring the continuity of essential government functions and protecting against mission degradation. A successful attack on the sector's assets could provide adversaries with a psychological victory by striking targets perceived to be very secure. The sector will continue to face risks from terrorist attacks, cyber security breaches, and ineffective security personnel procurement and oversight.

(U) Terrorist attack scenarios continue to represent significant risk to the Government Facilities Sector. A major challenge in the protection of government facilities is balancing security with the need for public access to government offices for services and transactions.[219] Global events and trends suggest, specifically, that terrorists will likely use VBIED tactics to attack U.S. critical infrastructure, and this tactic has historically represented one of the most successful methods of terrorist attack.[220] Government facilities can also be targeted by active shooters, as in the 2010 shooting at a Federal courthouse in Las Vegas.[221]

(U) The Government Facilities Sector will also face increased risk in the next several years from cyber intrusions into automated security and supervisory control and data acquisition systems. The increasing reliance on automated security systems will likely increase vulnerabilities and thus increase the likelihood of cyber intrusion,[222] especially in the form of sabotage by current or former insiders with malicious intent.[223] Cyber intrusion into the security systems of government facilities could compromise the protection of facilities, civil servants, and the general public and allow for exploitation and attacks with significant consequences.

(U) The Government Facilities Sector is critically dependent upon the Energy Sector, due to the energy needs associated with sustaining the vast number of facilities that provide essential government functions, and the Communications Sector, which provides telecommunication capabilities to government employees who perform duties within the sector domain. The Government Facilities Sector and the Transportation Systems Sector, Energy Sector, Communication Sector, Information Technology Sector, Dams Sector, and Emergency Services Sector are interdependent.

(U) Risks to the Healthcare and Public Health Sector

(U) The widespread and diverse Healthcare and Public Health Sector includes acute care hospitals; ambulatory healthcare; public-private financial systems; Federal, State, and local public health systems; disease surveillance; and private sector industries that manufacture, distribute, and sell drugs, biologics, and medical devices. [224] The Healthcare and Public Health Sector is vulnerable to a variety of threats and will continue to face risks from global supply chain disruptions, theft and exploitation of medical goods and confidential medical information, and pandemic disease. Such incidents could result in large numbers of illness and casualties, denial of service, or theft of confidential patient information.[225]

(U) The sector is at risk from vulnerabilities to global supply chain disruptions. Any event that leads to a shortage of a pharmaceutical, device, or biologic can be described as a supply chain disruption.[226,227] A natural disaster may make roads impassable and thereby prevent goods from arriving at an affected area or a product may be contaminated at its place of origin and need to be recalled, resulting in a limited amount of that product on the market. Independent of the reason, supply chain disruptions can be potentially catastrophic because health care providers tend to rely on just-in-time resupplying and therefore do not have sufficient stockpiles to weather a delay, especially during events that lead to an increased demand for healthcare.[228,229,230,231]

(U) The threat of theft and exploitation of medical goods and confidential medical information also presents an elevated risk to the Healthcare and Public Health Sector.

Theft and exploitation result from the work of malicious actors. The reasons for concern include the significant amount of radiological material used in civilian settings and the increasing dependence of the sector on computerized systems that house highly sensitive personal information.[232] Many medical facilities and laboratories contain radiological materials or biological select agents and toxins that are used for clinical treatment or medical research, and the open nature of medical facilities presents a potential security vulnerability.[233,234] These agents and materials may provide an attractive target to those wishing to construct a "dirty bomb," intentionally infect a population, or sell the material on the black market. Medical systems and vital records are also at risk for compromise or theft by external hackers or malicious insiders and present a trend in medical identity theft.[235,236,237]

(U) Experience with influenza demonstrated how a rapidly spreading infectious agent can significantly impact the Healthcare and Public Health Sector specifically and the country as a whole.[238,239,240] A naturally occurring agent like influenza was able to cause death, hospitalizations, and absenteeism.[241] Absenteeism is of particular concern for the sector because of the potential cascading consequences of not having a full complement of skilled healthcare personnel. If a more dangerous agent, such as smallpox, were to be released intentionally, the effects could be even more catastrophic due to the increased lethality and general immunological naiveté to the disease.[242]

(U) All sectors are dependent on the Healthcare and Public Health Sector to provide healthcare services to their workforces in order to sustain operations. The sector is critically dependent on the Transportation Systems Sector; the Postal and Shipping Sector, which provides movement of supplies, raw materials, pharmaceuticals, personnel, emergency response units, and patients; the Communications Sector; the Information Technology Sector; the Energy Sector; the Water Sector; the Food and Agriculture Sector, which provides essential services for daily business operations; and the Chemical Sector, which directly supplies the pharmaceutical industry. The Healthcare and Public Health Sector is interdependent with the Emergency Services Sector, coordinating with first responders and emergency medical services as well as using local law enforcement for security and legal enforcement of health regulations, such as quarantines.[243]

(U) Risks to the Information Technology Sector

(U) The Information Technology (IT) Sector is a functions-based sector that provides products and services to enable the private and public sectors to execute their key missions. Critical Information Technology Sector functions include producing and providing IT products and services; providing incident management capabilities; providing domain name resolution services; providing identity management and

associated trust support services; providing Internet-based content, information, and communications services; and providing Internet routing, access, and connection services.[244] The sector will continue to face risks from cyber exploitation of supply chain vulnerabilities and cyber exploitation of identity resources.

(U) The sector is at risk from cyber threats, particularly those that degrade the confidentiality, integrity, or availability of the critical functions. Depending on its scale, a cyber attack could be debilitating to the Information Technology Sector's highly interdependent critical infrastructures and ultimately to our economy and national security.[245] These cyber risks include the unintentional (e.g., the accidental disruption of Internet content services) and intentional (e.g., exploitation of IT supply chain vulnerabilities or the breakdown of Internet interoperability due to attack).

(U) Other sector risks stem from deliberate attacks that target Internet-based identity management, content, information, and communications. For example, malicious code increasingly proliferates through social networking and can degrade IT systems' functionality, and a successful network compromise from a spear-phishing attack only requires victimizing a user with access to just a limited network or administrative resources to lead to data breaches and associated financial and reputational costs.[246]

(U) While the Information Technology Sector provides functions that enable all sectors, the sector is critically dependent upon the Communications Sector and the Energy Sector. The Information Technology Sector, Banking and Finance Sector, Chemical Sector, Healthcare and Public Health Sector, Transportation Systems Sector, and Water Sector are interdependent.[247]

(U) Risks to the National Monuments and Icons Sector

(U) The National Monuments and Icons Sector is committed to ensuring that the symbols of the Nation remain protected and intact for future generations. The symbolism and international recognition of many National Monuments and Icons Sector assets make them appealing targets to al-Qa'ida and other adversaries, and their inherent openness makes them vulnerable to attack.[248] The sector faces current and increasing risks due to terrorist attacks and cyber intrusion.

(U) The threat of terrorist attack represents significant risk to the National Monuments and Icons Sector. Global events and trends suggest, specifically, that terrorists will likely use VBIED tactics to attack U.S. critical infrastructure.[249] Al-Qa'ida and its affiliates have demonstrated proficiency for conducting attacks using explosives, and VBIEDs have historically represented one of the most successful methods of terrorist attack.[250]

Furthermore, some sector assets have little standoff distance from major roadways and are vulnerable to VBIEDs. In addition, other sector assets, specifically in the National Capital Region, are in close proximity to one another, which could result in increased fatalities and injuries if an attack were successful. Scenarios involving lone shooters, hazardous materials, or aircraft as a weapon are also representative of the terrorism risk to the sector.[251]

(U) Overall risk to the NMI Sector is also affected by access issues attributed to insufficient technology acquisition and strategic human capital management.[252] While icon and park officials have acquired a number of technologies to enhance the security of their assets, they have no guidance for evaluating the cost-effectiveness among countermeasure alternatives. While the Gateway Arch and Statue of Liberty have modernized their dispatch and screening technologies in recent years, breaches continue to occur since the security improvements. Furthermore, officials from both icons have stated a need for guidance in investing in technology.[253] A 2009 GAO report also found that human capital management at icons lacks a security focus, with physical security coordinators often lacking the appropriate experience or expertise. These security officials also face challenges in receiving the necessary physical security and critical infrastructure protection training from Federal resources.[254]

(U) The National Monuments and Icons Sector is critically dependent on the Government Facilities Sector, due to the interconnected nature and geographic proximity of assets, especially in the National Capital Region; and both the Emergency Services Sector and Communications Sector, due to the presence large crowds and the use of assets service providers for risk mitigation and incident response activities. Most National Monuments and Icons Sector assets do not have interdependencies with other sectors and are not a critical component to the operation of other sectors.[255]

(U) Risks to the Nuclear Reactors, Materials, and Waste Sector

(U) The Nuclear Reactors, Materials, and Waste Sector is composed of nuclear power plants; research and test reactors; fuel cycle facilities; radioactive waste management; decommissioning reactors; nuclear and radioactive materials used in medical, industrial, and academic settings; and nuclear material transport. The sector maintains a high standard for preparedness, but a physical or cyber attack could lead to serious public health, environmental, psychological, or economic consequences.[256] The sector faces two general categories of risk: risk to facilities and risk to materials.

(U//FOUO) Facilities can be put at risk by physical incidents (attack, sabotage, accident, or a natural disaster) or cyber intrusions into a facility's industrial control systems, which could potentially cause physical repercussions.[257] Onsite storage of large quantities of

spent reactor fuel at almost every U.S. reactor site greatly increases the potential consequences of a terrorist attack or natural disaster on a plant and its surroundings.[258] If successfully attacked or disrupted, some nuclear facilities have the potential to release radioactive material into the environment. As in other sectors, an insider threat could increase likelihood of success, as is reflected in the Nuclear Regulatory Commission's design basis threat.[259] The Stuxnet worm highlighted the persistent cyber risk and demonstrated the new potential for seizing control of industrial control systems.[260]

(U) The sector also faces risk to materials, both from the threat of theft and diversion of nuclear and radioactive materials and the vulnerability to disruptions of the supply chain. Sector radioactive materials, including nearly 55,000 high-activity[jj] sources, are used in a range of industrial, medical, and other commercial settings.[261] Determined adversaries could use stolen radioactive materials as elements of radiological dispersal devices or radiation exposure devices. Disruption of the supply chain for commercial radioisotopes and other materials also poses an ongoing risk. This was demonstrated last year, when reliance on aging, overseas reactors triggered a global shortage of molybdenum-99 (Mo-99), a radionuclide that decays to a form used in millions of medical procedures performed annually in the United States.[262]

(U) The Nuclear Reactors, Materials, and Waste Sector is critically dependent on the Energy Sector as a supplier of electrical power; the Water Sector, for cooling of nuclear reactors; the Transportation Systems Sector, regarding movement of nuclear and radioactive material; Chemical Sector, regarding hazardous chemicals used at fuel cycle facilities; Healthcare and Public Health Sector, regarding nuclear medicine; Emergency Services Sector, regarding response capabilities; and Government Facilities Sector, regarding Federal and State facilities that use radioactive material.[263]

(U) Risks to the Postal and Shipping Sector

(U) The Postal and Shipping Sector is an integral component of the U.S. economy, employing more than 1.8 million people and earning direct revenues of more than $213 billion per year.[264] The Postal and Shipping Sector moves more than 720 million messages, products, and financial transactions each day.[265] The sector is highly concentrated, with a handful of providers holding roughly 94 percent of the market share.[266] The sector faces risks from the threat of mail-based IEDs; the threat of terrorist attacks using chemical, biological, radioactive, nuclear and explosive (CBRNE)

[jj] (U) The high-activity sources cited here are Category 1 and 2 sources as defined in the International Atomic Energy Agency's Code of Conduct on the Safety and Security of Radioactive Sources. [www-pub.iaea.org/MTCD/publications/PDF/Code-2004_web.pdf, accessed on June 16, 2011]

weapons or agents; and the vulnerability of the sector's openness, which allows for anonymous entry points for attacks.

(U) The sector maintains an extremely large number of collection points at which parcels and letters can be inserted for delivery to ensure ease of access to and use of the system for its customers.[267] These collection facilities present a vast array of relatively anonymous entry points at which terrorists could insert dangerous materials for delivery to intended targets.[268] Further, the sector is a highly trusted entity, and its employees and representatives have ready access to businesses and residences throughout the country.

(U) This combination of ubiquitous, trusted personnel access to other sectors, an extraordinary number of anonymous insertion points, and the potential for delivery to diverse recipients makes the Postal and Shipping Sector attractive to terrorists, who may use it to attack persons or critical infrastructure in other sectors. Greek and Italian anarchists demonstrated this capability in 2010 and 2011 parcel-based attacks in Europe.[269,270] In October 2010, explosives artfully concealed in packages from Yemen destined for the United States were found both already in transit and ready for transit, resulting in acute attention and immediate policy changes in inbound international mail.[271] Such changes affected the flow of air mail, causing delays in service.[272]

(U//FOUO) The sector's risk is also raised by the threat of hazardous materials, including CBRNE agents. The Postal and Shipping Sector is one of the few that has been threatened by biological agents: the U.S. Postal Service (USPS) was used as a vehicle for delivering anthrax in 2001.[273] In the aftermath of the anthrax attacks in 2001, USPS projected that the subsequent declines in mail volume and revenue could affect the agency's bottom line by as much as $2 billion that fiscal year.[274]

(U) The Postal and Shipping Sector is critically dependent on the Transportation Systems Sector for the movement of mail and packages by air, road, or rail; Energy Sector for power; and Information Technology Sector and Communications Sector for supporting logistics operations and automatic identification and sorting.[275]

(U) Risks to the Transportation Systems Sector

(U) The Transportation Systems Sector is a vast, open, accessible, interconnected system that moves millions of passengers and millions of tons of goods.[276] In addition to physical and cyber threats from terrorists, natural and industrial disasters also have the potential to impact the sector. The risk mitigating actions necessary for the sector are diverse, reflecting the complexity of the transportation network and the varied elements

that pose risks. The Transportation Systems Sector consists of six modes: aviation,[kk] highway,[ll] mass transit,[mm] maritime, pipeline systems,[nn] and freight rail.[oo] The aviation mode faces the highest risk for the sector, followed by mass transit.[pp]

(U) Despite security enhancements since the attacks on September 11, 2001, intelligence continues to indicate that aviation remains the top target of terrorists.[277] Attempts such as the December 25, 2009, attack on Northwest Flight 253[278] support this claim. The detonation of an IED during a flight is now the foremost threat to airlines.[279]

(U) The mass transit system features an inherently open environment designed to make it easily accessible to the public. While these characteristics facilitate the rapid transport of people, they also provide opportunities for terrorists to stage attacks, increasing the risk of attacks targeting the mode. Terrorists have demonstrated the capability to attack mass transit systems abroad, as evidenced by the attacks on subway and rail systems in Minsk (2011),[280] Moscow (2010),[281] Mumbai (2008),[282] London (2005),[283] Moscow (2004),[284] and Madrid (2004).[285]

(U) The Transportation Systems Sector is an integrated network of interconnected systems, dependent on critical and noncritical infrastructure sectors alike for both daily operations and long-term viability. The Transportation Systems Sector is critically dependent on the Information Technology Sector. The Transportation Systems Sector, Energy Sector, Government Facilities Sector are interdependent.

[kk] (U) The aviation mode includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional airfields. This mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.
[ll] (U) The highway mode encompasses more than 4 million miles of roadways and supporting infrastructure. Vehicles include automobiles, buses, motorcycles, and all types of trucks.
[mm] (U) The mass transit mode includes multiple-occupancy vehicles, such as transit buses, trolleybuses, vanpools, ferryboats, monorails, heavy (subway) and light rail, automated guideway transit, inclined planes, and cable cars designed to transport customers on local and regional routes.
[nn] (U) The pipeline systems mode includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the Nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals.
[oo] (U) The freight rail mode consists of hundreds of railroads, more than 143,000 route-miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives.
[pp] (U) The Transportation Security Administration and the Coast Guard do not have a position on where risks to Maritime lay in comparison with those of the other modes.

(U) THE MARINE TRANSPORTATION SYSTEM

(U) The Marine Transportation System (MTS) is a complex system that is both geographically and physically diverse in character and operation. It consists of about 95,000 miles of coastline, 361 ports, over 25,000 miles of navigable waterways, 3.4 million square miles of Exclusive Economic Zone to secure, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water. This part of the Transportation Systems Sector is at risk for potential cyber intrusion, port vulnerability, and insecure intermodal shoreside connections..

(U) Cybersecurity has become increasingly important as the MTS has become increasingly dependent on cyber systems and faces a growing risk from cyber attacks. These systems are used for a variety of purposes, including access control, navigation, traffic monitoring, and information transmission. Although the interconnectivity and utilization of cyber systems facilitate transport, they can also present opportunities for the exploitation of the MTS.

(U) Ports are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks.[a] Port infrastructures are vulnerable to intrusion and even though a robust security plan system, which includes domestic facilities and vessels as well as foreign vessels that call into the United States, has been implemented through the Maritime Transportation Security Act (MTSA), if successfully attacked, it would pose a risk for catastrophic consequences. Port facilities, along with the ships and barges that transit port waterways, are especially vulnerable to tampering, theft, and unauthorized persons gaining entry to collect information and commit unlawful or hostile acts.[a] Due to just-in-time methods, a successful attack against one node of maritime infrastructure could disrupt entire systems, cause congestion, limit capacity for product delivery, cause significant damage to the economy, or create an inability to project military force.[a] Risks related to small vessel security continue to be a focus for the U.S. Coast Guard.

(U) The MTS faces additional risk from the potential disruption of intermodal connections. As a network of maritime operations, the MTS interfaces with shoreside operations at intermodal connections as part of overall global supply chains or domestic commercial operations.[a] Across the Transportation Systems Sector as a whole, intermodal terminals are potentially high-value targets for adversaries because the large volume of cargo can lead to significant loss of life and economic disruption.[a] Much like port facilities, the disruption of intermodal connections could have cascading consequences due to just-in-time methods and an increasingly complex supply chain.

(U) Risks to the Water Sector

(U) The Water Sector is composed of over 153,000 public drinking water systems and approximately 16,500 publicly owned wastewater treatment utilities. These utilities consist of source waters, treatment facilities, pumping stations, storage sites, and extensive distribution, collection systems, and monitoring systems.[286] The sector faces risk from the terrorist use of chemical, biological, or radiological (CBR) agents to contaminate water supplies; natural hazards; and physical and cyber attacks. Successful attacks on a drinking water or wastewater system could result in large numbers of illness, casualties, and denial of service, which could severely impact the Nation's public health and economic vitality.[287]

(U) A key risk of concern for the Water Sector is the terrorist use of CBR to contaminate a drinking water system, whether by accidental or intentional means. Most public water supplies are monitored and treated to prevent the distribution of contaminated drinking water.[288,289] The risk of terrorist CBR contamination stems from both the enduring terrorist threat to contaminate the U.S. water supply and the serious health impacts that

could result from an undetected contaminant.[290,291,292,293] These impacts could vary depending on the type of substance, route of exposure (ingestion, absorption, inhalation), and amount of time before the contaminant is detected.[294]

(U) Natural hazards, such as hurricanes, tornadoes, floods, earthquakes, and drought, pose a serious and continuing risk for the sector.[295,296] Water infrastructure may be severely disrupted or destroyed by such hazards, which may further complicate an overall disaster emergency response due to multiple cross-sector interdependencies.[297,298] Critical water shortages may also result from drought conditions and climate change, leading to water use restrictions and rationing.[299,300]

(U) Physical and cyber attacks on critical water infrastructure by terrorists, homegrown extremists, or disgruntled insiders also present important risks to the Water Sector.[301] Physical attacks using IEDs or VBIEDs on chemical storage tanks or other critical nodes in a drinking water or wastewater system could result in the release of hazardous materials or in a long-term loss of service should a "single-point-of-failure" be destroyed.[302] Cyber attacks and intrusions on supervisory control and data acquisition systems or other business systems pose a serious threat to the Water Sector, allowing malicious actors to manipulate or exploit control systems essential to operation of drinking water and wastewater utilities.[303,304,305]

(U) The Water Sector is critically dependent upon the Energy Sector, as a loss of power can disrupt pumps and treatment operations, which can result in a loss of potable drinking water or properly treated wastewater for an entire community; Chemical Sector, as chemicals such as chlorine are used to disinfect and treat drinking water and wastewater; and Critical Manufacturing Sector, for the supply of certain utility components. Repair of damaged infrastructure could, in some cases, be prolonged as specialized replacement equipment is obtained and installed.[306] Disruptions to the Water Sector resulting in prolonged service interruptions to dependent or interdependent assets and other critical customers, such as the Energy Sector,[307] Chemical Sector, Information Technology Sector, Healthcare and Public Health Sector, Banking and Finance Sector, and Food and Agriculture Sector, would likely have far-reaching negative public health, economic, and psychological impacts.[308]

(U) Regional Risks

(U) Critical infrastructure throughout the United States experiences naturally occurring and manmade risks related to the unique characteristics of various regions, as well as the sectors and the cross-cutting risks described above. Risks that have potentially significant impact in the critical infrastructure context are presented in the 2011 National Risk Profile in terms of the Federally administered/Federal Emergency Management Agency (FEMA) regional construct along with a discussion of those geographic risks that affect more than one region (e.g., tornado risk). There may be cases where the national risks may not be as great to a particular region but still create cross-cutting risk. National risks that could potentially affect particular regions will only be discussed in this section if from the perspective of the region those cross-cutting risks are considered amongst the most significant.

(U) Risks to Federally Administered Region I

(U) Region I is composed of Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. Risks to the Energy Sector and the Transportation Systems Sector are of greatest concern to this region. Since 1998, FEMA has issued 65 Federal disaster declarations for the States within the region.[309] Severe storms, including snow and ice storms, are the costliest natural hazards to the region,[310] accounting for over 95 percent of the Federal funds issued for recovery and response efforts in the region during this time.[311] The region's most common natural hazards are severe winter weather, hurricanes, and other storms that can cause flooding throughout the region.[312]

(U) Severe winter storms have historically tested the resilience of the region's critical infrastructure. The largest winter storm in recent history was the 1978 blizzard that saw snowfall totals from 20 to 40 inches across the Northeast.[313] This storm caused $500 million of damage in Massachusetts alone.[314] A December 2010 blizzard halted regional transportation, including important aviation and rail networks in Massachusetts and Rhode Island.[315] The following month another blizzard struck Massachusetts, this time with energy and communications cut off to several towns.[316] Rural areas, such as in Maine, New Hampshire, and Vermont, are at greater risk of losing power and becoming isolated during a winter storm[317] because snow clearing and power restoration efforts take much more time in rural areas than along highways and in urban areas.[318]

(U) Though not as common as severe winter storms, hurricanes potentially can cause as much or greater damage to critical infrastructure in the region. Since 1900, 39

tropical systems have impacted New England – 25 were hurricanes, while 14 were tropical storms.[319]

(U) Transportation-related delays cost about $1.7 billion annually, with all 6 States in the region counted among the top 15 with the most structurally deficient and obsolete bridges in the country.[320] Increasing the Transportation Systems Sector's connectivity to Boston will continue to be a major goal for the region since Boston accounts for almost 40 percent of the region's gross domestic product,[321] as well as a great deal of traffic. New investments were made in the region's transportation infrastructure with $2 billion in Federal funding for high-speed rail from the Department of Transportation.[322] Much of this investment will go directly to States in the region to support rail projects along the Northeast Corridor and throughout the Northeast.[323] Although this investment should reduce risk by decreasing vulnerability in the rail system, rail and other elements of the Transportation Systems Sector in the region remain at risk.[324] Also, given the expressed interest of al-Qa'ida in targeting trains in the United States and throughout the world,[325] threats to the rail subsector create additional regional risk.

(U) Reducing risk to and ensuring resilience of the Energy Sector, especially during winter storms and summer heat waves, is critical to the region's economy. Although the region was spared the worst of the summer 2003 Northeast blackout, Connecticut, Massachusetts, and Vermont still incurred approximately $100 million in combined economic damages.[326] New England's all-time electricity consumption record for one month was recorded in July 2010, and new peak demand records were set for the months of May and September that year.[327] Despite significant and increasing energy demands in the region and throughout the Nation, very little new energy generation has been emplaced in the region.[328] Further, 620 megawatts per day from the Vermont Yankee nuclear plant could be taken offline in March 2012 pending the outcome of a dispute between Vermont and the Nuclear Regulatory Commission, potentially exacerbating the problem.[329] Times of emergency and peak demand driven by extreme weather conditions could increase vulnerability for the Energy Sector, placing the region at greater risk.

(U) From 1998 to 2009, there were five terrorist attacks in the region.[330] Three of these were bombing/explosive attacks and were directed against private citizens, private property, or a government facility.[331] The threat of terrorism creates significant risk for the region. Given the importance of energy and transportation in these States, and the dependence of the Transportation Systems Sector on the Energy Sector, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Defense Industrial Base Sector, Nuclear Reactors, Materials, and Waste Sector, and Transportation Systems Sector.[332]

(U) Risks to Federally Administered Region II

(U) Region II is composed of the States of New Jersey and New York and the territories of Puerto Rico and the U.S. Virgin Islands. Risks to the Banking and Finance and Transportation Systems Sectors are of greatest concern in this region. Since 1998, FEMA has issued 58 Federal disaster declarations for the States and territories within the region.[333] Severe storms, including snow and ice storms, are the costliest natural hazards to the region.[334] Almost 80 percent of the Federal funded recovery and response efforts in the region during this period addressed the terrorist attacks of September 11, 2001.[335] When this is taken out of consideration, severe storms account for approximately 90 percent of the Federal funds issued for response and recovery efforts.[336]

(U) Snowstorms and severe winter weather occur frequently in New York and New Jersey, and Puerto Rico and the U.S Virgin Islands are often threatened by hurricanes. This severe and often extreme weather creates economic vulnerability and risk to the region. However, given the location of New York geographically and the position of many nationally significant assets within New York City, extreme weather creates the greatest risk for New York. Based on historical frequency, New York City can expect a major snowstorm of 16 inches or more, approximately every nine years.[337] Roads and bridges are especially vulnerable to these storms.[338] Snow hazards also create consequences, such as transportation accidents and disruptions, that are especially costly to New York City, increasing risk to the city and this part of the region. Large snow removal costs; lost revenue from retail businesses, parking meters, and towing; and other factors that affect local and State budgets, such as paying snow-related claims and police overtime, are all significant consequences. It is estimated that during the winter of 1995-1996, these cost New York City $2.3 billion and the metropolitan region $4.9 billion.[339]

(U//FOUO) Reducing risk to and ensuring resilience of the Banking and Finance Sector in New York is critical to the Nation's economy. The Lower Manhattan Financial District (Wall Street) accounts for 40 percent of the country's financial industry and is as an important symbol of U.S. economic power.[340] Osama bin Laden indicated that the World Trade Center in New York was targeted on September 11, 2001, for economic reasons.[341] Khalid Sheikh Muhammad also plotted against the New York Stock Exchange and several other financial targets in the region to hurt the Nation's economy.[342] Threats and consequences have been, and are expected to remain, high for this sector, placing this part of the region and the Nation at continued risk.

(U//FOUO) Given that New Jersey and New York are global transit hubs, the viability of the Transportation Systems Sector is critical to the region, the Nation, and the world. The New York City metropolitan area possesses major ports, airports, bridges, and tunnels, as well as the highest concentration of mass transit assets in the country, serving more than 2 billion passengers per year.[343] These assets have been targeted frequently by terrorists since September 11, 2001, such as with the Najibullah Zazi plot to attack the New York subway in 2009 and the al-Qa'ida plot to attack U.S. rail systems on the tenth anniversary of September 11, 2001, following the raid on Osama bin Laden's compound in Pakistan.[344] Attacks on transportation in and connecting to New York City could yield large numbers of casualties, interrupt services, instill fear, and necessitate costly and prolonged recovery efforts.[345]

(U) The threat of terrorism creates significant risk for the region. The terrorist attack on September 11 was a major terrorist event, but only 1 of 22 terrorist attacks that occurred in this region from 1998 to 2009.[346] Twenty of these attacks took place in New York. Therefore, the threat to New York has been greater than to the rest of the region, placing the State at the greatest risk.[347] Both New Jersey and New York possess major ports of entry, with the ports of entry in Puerto Rico and the U.S. Virgin Islands perhaps taking on greater significance in that entry into these territories may be easier than into any of the country's States and facilitate easier access into the rest of the Nation. As of February 2010, al-Qa'ida had identified New York City among a number of important cities where attacks should occur. Given the importance of banking, finance, tourism, and transportation in and for these States and territories, and the dependence of the Transportation Systems Sector on the Banking and Finance Sector, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region. Also, although regional collaboration is becoming more critical to address the terrorist threat (including that posed by homegrown violent extremism),[348] the composition of the region with two States and two territories separated by great distances makes such collaboration difficult. This lack of collaboration itself represents a significant vulnerability that contributes to regional risk.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Defense Industrial Base Sector, Transportation Systems Sector, and Water Sector.[349]

(U) Risks to Federally Administered Region III

(U) Region III is composed of Delaware, Maryland, Pennsylvania, Virginia, West Virginia, and the District of Columbia.[350] Risks to the Government Facilities Sector and Transportation Systems Sector are of greatest concern to this region. Floods, hurricanes, severe storms, snow, and tornadoes all create risk for the region. Since 1998, FEMA has issued 72 major disaster declarations for the regional States and the District of Columbia.[351] Severe storms are the costliest natural hazards to the region, accounting for 46 percent of the Federal funds issued for recovery and response efforts during this time.[352] Hurricanes accounted for 37 percent, followed by snow, floods, and tornadoes.[353]

(U) Severe storms pose an ongoing, high-frequency risk to this region and are responsible for 41 of the 68 major disaster declarations since 1999.[354] Severe storms can create extensive disruptions in the Energy Sector, as seen in the July 2010 storms, which cut power to more than 250,000 residents in the Washington, DC metropolitan area.[355] Severe storms can also create compound risk, as seen with the blizzard of February 2010 that affected energy services, transportation, and the Government, disrupted power for 218,000 residents,[356] caused nearly 1,500 car accidents in Virginia alone,[357] and forced the closure of the Federal Government for five days at a cost of $355 million.[358]

(U//FOUO) The Transportation Systems Sector is critical to the region owing to its heavy dependence on mass transit. The Washington Metro transit system carries more than 200 million passengers annually,[359] and homegrown extremists have repeatedly shown interest in targeting it, with two separate arrests occurring in 2010.[360,361] Amtrak, the nation's busiest passenger rail line, transits through the Northeast Corridor, passing through Delaware, the District of Columbia, Maryland, and Pennsylvania.[362] Given the expressed interest of al-Qa'ida in targeting trains in the United States and throughout the world,[363] threats to the rail subsector create additional regional risk.

(U) From 1998 to 2009, there were 15 terrorist attacks in the region, including the terrorist attack on September 11.[364] Four of these were facility/infrastructure attacks, two of which were directed at businesses.[365] The symbolic value of the District of Columbia—as a major city[366] as well as the Nation's Capital and the location of headquarters elements for all of the Federal departments and agencies—makes it a high-value target and creates greater risk for the Government Facilities Sector within the region. The District of Columbia, Maryland, Virginia, and West Virginia have high concentrations of Government Facilities assets. Sector assets in the Washington

metropolitan area have been attacked or targeted in the past, such as with the September 11 attack on the Pentagon in Virginia and a 2010 plot to bomb a Maryland military recruiting center.[367] The Delaware River shoreline south of Philadelphia also has one of the largest concentrations of industrial facilities, oil refineries, and petrochemical plants in the world, making it a high-value target as well.[368] Many national monuments and icons are also found within the District of Columbia and in other States throughout the region, including the Liberty Bell in Pennsylvania. The threat of terrorism creates significant risk for the region. As of February 2010, al-Qa'ida had identified Washington, D.C. among a number of important cities where attacks should occur. Given the importance of government, national monuments and icons, and transportation in the region, the threat of a terrorist attack on the Government Facilities Sector, National Monuments and Icons Sector, or Transportation Systems Sector creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Defense Industrial Base Sector, Government Facilities Sector, and Transportation Systems Sector.[369]

(U) Risks to Federally Administered Region IV

(U) Region IV is composed of Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee.[370] Risks to the Commercial Facilities Sector and the Chemical Sector are of greatest concern to this region. Since 1998, FEMA has issued 161 disaster declarations for the States within the region.[371] Hurricanes are the costliest natural hazards to the region, accounting for more than 83 percent of the Federal funds issued for recovery and response efforts during this time.[372] Severe storms accounted for another 12 percent, with the remainder provided in response to ice storms, coastal storms, tornadoes, snow, and fires, ranked by funding.[373] The region's most common natural hazards are hurricanes, tornadoes, flooding, ice storms, and wildfires.[374] Western Tennessee and Western Kentucky lie within the New Madrid Seismic Zone, where some of the largest earthquakes in North America have occurred historically.

(U) Hurricanes and tropical storms continue to pose a high-frequency, high-consequence risk to this region, responsible for 42 of the 141 major disaster declarations and 22 of the 27 Federal emergency declarations since 1999.[375] Twenty-eight of these declarations involved hurricanes and tropical storms.[376] Hurricanes can cause significant damage to the region's critical infrastructure, especially given the proximity to the coast of many of its major population centers, thereby contributing to the region's risk. Catastrophic consequences were created by Hurricanes Katrina and Rita in 2005, leading to the deaths of more than 1,800 people, more than $200 billion in damages, and impacting Alabama, Florida, Louisiana, and Mississippi.[377]

(U) The Commercial Facilities Sector is an important driver of the regional economy and is at higher risk. Assets in this sector are highly visible, are easily accessible, have the potential to result in mass casualties if attacked or otherwise destroyed, are symbolically important (as at major sporting events), and are of interest to terrorists, having been attacked previously. Open access counters the deterrence provided by security barriers at these facilities, making the sector more vulnerable to attacks[378] and increasing risk for the region. Events featuring mass gatherings that take over large areas of land and become small cities—such as NASCAR races in Alabama, Florida, Kentucky, North Carolina, South Carolina, and Tennessee—possess unique vulnerabilities that create risk.[379] Terrorist attacks on commercial facilities in the region have occurred in the past, including the Atlanta Olympic Park bombing in Georgia in 1996. Commercial facilities are also vulnerable to the use of firearms, as seen in shooter incidents that occurred at retail locations in Florida, Georgia, South Carolina, and Tennessee from 2004 to 2008.[380]

(U//FOUO) Natural hazards put the Chemical Sector at risk in the region. Chemical assets are numerous in the region, and many are located along the coasts. Hurricanes can result in the loss of power, as well as wind and water damage, all of which can disrupt chemical assets.[381] Even plants undamaged by hurricanes can take up to four weeks to restart operations until inspections are conducted and those utilities necessary for chemical facilities to function recover.[382] Issues with the Chemical Sector greatly impact other sectors upon which it is dependent or with which it is interdependent. For example, following Hurricane Katrina, reductions in the availability of feedstock impacted transportation infrastructure, and higher energy prices impacted petrochemical production.[383]

(U) From 1998 to 2009, there were 37 terrorist attacks in the region. Twenty-three of these were facility/infrastructure attacks. [qq] Florida experienced the highest number of attacks—24 of the 37—as well as 18 of the region's 23 facility/infrastructure attacks.[384] The threat of terrorism creates significant risk for the region. Given the importance of commercial facilities and chemical assets in these States, the threat of a terrorist attack on either or both of these sectors (such as where assets in both sectors are located near each other) creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Defense Industrial Base Sector, Food and Agriculture Sector, and Transportation Systems Sector.[385]

[qq] (U) The Global Terrorism Database defines a facility/infrastructure attack accordingly: "An act, excluding the use of an explosive, whose primary objective is to cause damage to a non-human target, such as a building, monument, train, pipeline, etc. Such attacks consist of actions primarily aimed at damaging property, or at causing a diminution in the functioning of a useful system (mass disruption) yet not causing direct harm to people. Such attacks include arson and various forms of sabotage. Can include acts that intend to cause harm to people as a result of the harm done to objects (e.g., blowing up a dam so that the ensuing flood will kill residents downstream). Can include acts which aim to harm an installation, yet also cause harm to people incidentally." [START, "GTD Variables & Inclusion Criteria, May 2010, www.start.umd.edu/gtd/downloads/Codebook.pdf, accessed 23 May 2011]

(U) Risks to Federally Administered Region V

(U) Region V is composed of Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin. Risks to the Food and Agriculture Sector—especially with respect to the dairy industry—and the Transportation Systems Sector are of greatest concern to this region. Since 1998, FEMA has issued 87 Federal disaster declarations for the States within the region.[386] Severe storms are the costliest natural hazards to the region, accounting for approximately 73 percent of the Federal funds issued for recovery and response efforts during this time.[387] The region's most common natural hazards are flooding, severe storms, and tornadoes,[388] with Minnesota and Wisconsin accounting for most of the flooding.[389]

(U) Due to the region's geography along the Mississippi River, which begins in Minnesota, flooding is a perennial threat to the region. In 2011, the region's snowpack contained a water content ranked among the highest of the last 60 years and led to flooding along the length of the Mississippi River.[390] The record setting Mississippi River flood of 1993 disrupted transportation and industry along the Mississippi for months, with severe impacts to surface and river transportation.[391] The flood was responsible for an estimated $15 to $20 billion in economic damages, making it one of the worst floods ever in the United States.[392]

(U) The Food and Agriculture Sector is critical to the region. Wisconsin ranked second, Minnesota ranked sixth, and Michigan ranked eighth in 2010 for milk production in the Nation.[393] Illinois, Minnesota, Wisconsin, and Indiana also ranked among the Nation's top 10 States in terms of total agricultural commodities sales in 2007.[394] Threats to food and agricultural production contribute to risk in the region. The Food and Agriculture Sector in the region is also dependent upon the Transportation Systems Sector (particularly the navigable waterways and inland maritime transportation infrastructure) as much of the grain transported downstream on the Mississippi and Illinois Rivers is grown in Illinois, Minnesota, Ohio, and Wisconsin.[395] Therefore, natural hazards and other threats to and vulnerabilities within the Transportation Systems Sector also increase risk for the Food and Agriculture Sector, as well as for the region.

(U//FOUO) The region's Transportation Systems Sector serves a vital role linking the country together. The region is at the center of the national rail network with Chicago serving as one of the largest rail gateways in the United States.[396] More than 50 railroads provide service from Illinois to every part of the continental United States.[397] Disruption of several key intermodal facilities would likely increase transportation costs significantly.[398] In the Maritime subsector, the Port of Chicago plays a vital role

connecting the Great Lakes to the Mississippi River, moving more than 26 million tons of goods annually. The large volume of traffic over an expansive area that continues down the Mississippi River presents a vulnerability and security challenge.[399]

(U) Terrorist attacks have also occurred in the region. From 1998 to 2009, there were 32 terrorist attacks in the region.[400] Twelve of these were facility/infrastructure attacks. Threats to the Transportation Systems Sector also contribute greatly to the risk. As of February 2010, al-Qa'ida had identified Chicago among a number of important cities where attacks should occur. Chicago, the most populous city in the region, is also home to the Nation's third busiest rapid rail transit system[401] and the world's fifth busiest airport.[402] The December 2009 attempt to detonate an explosive during an international flight bound for Detroit[403] and the confirmation that al-Qa'ida still seeks to attack mass transit in the United States[404] indicate that the Nation's adversaries will probably continue to try to exploit real and perceived vulnerabilities in the region's transportation system, thereby increasing risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Food and Agriculture Sector, and Transportation Systems Sector.

(U) Risks to Federally Administered Region VI

(U) Region VI is composed of Arkansas, Louisiana, New Mexico, Oklahoma, and Texas. Risks to the Chemical Sector, Commercial Facilities Sector, and Energy Sector are of greatest concern in this region. Since 1998, FEMA has issued 101 Federal disaster declarations for the States within the region.[405] Hurricane Katrina, which made landfall in Louisiana on August 29, 2005, is the single most devastating natural disaster for the region and the most costly U.S. hurricane on record, resulting in $81.1 billion in property damages alone.[406] Hurricanes are the costliest natural hazard to the region, accounting for nearly 75 percent of Federal funds issued for recovery, response, and mitigation efforts during this time. Nearly all of the remaining 25 percent of Federal funds were spent to recover from coastal storms, ice storms, and severe storms. The region's most common natural hazards are coastal storms, hurricanes, severe ice storms, and severe storms.

(U) The geography of the region, particularly where Louisiana and Texas meet the Gulf of Mexico, makes the region vulnerable to coastal storms and hurricanes. Hurricanes can cause significant damage to critical infrastructure in the region, especially to the gas, oil, and petrochemical infrastructure assets clustered along the Gulf Coast in Lake Charles, Louisiana, and Houston, Texas. These two clusters account for approximately 20 percent of U.S. petroleum refinery operable capacity.[407] Hurricane Katrina caused damage and destruction to 30 oil platforms and forced 9 refineries to shut down throughout the region.[408] Thus, the risk to the region's energy industry significantly increases during the summer hurricane season.

(U) The Commercial Facilities Sector is an important driver of the regional economy and is at higher risk. Commercial facilities in the region, including entertainment complexes and buildings with many business and governmental tenants in urban areas like New Orleans, Dallas, Houston, and San Antonio are just a few examples of the many high-value commercial facilities. Events featuring mass gatherings that take over large areas of land and become small cities, such as the Texas State Fair (the largest in the country) and NASCAR races in Texas possess unique vulnerabilities that create risk.[409] Assets in this sector are highly visible, are easily accessible, have the potential to result in mass casualties if attacked or otherwise destroyed, are symbolically important (as at major sporting events), and are of interest to terrorists, having been attacked previously. Open access counters the deterrence provided by security barriers at these facilities, making the sector more vulnerable to attacks[410] and increasing risk in the region. The FBI foiled a plot in 2009 by Jordanian Hosam Smadi to blow up the Fountain Place Building (known for its unique and artistic architecture and housing a large number of

public and private sector offices, including financial institutions) in Dallas.[411] Smadi, radicalized through the Internet and trying to imitate the events of September 11, sought to bring down a notable skyscraper and kill thousands of people. Due to the visibility and economic value of many of these assets, the threat to commercial facilities remains high and contributes to risk in the region.

(U) Industrial disasters have also occurred in this region. The incident involving the Deepwater Horizon oil drilling rig occurred off the Louisiana coast on April 20, 2010, creating the largest offshore oil spill in U.S. history.[412] Currently, total losses are in excess of $40 billion,[413] not including the cost of cascading effects involving other critical infrastructure sectors in the region.[414] A number of human factors are thought to have contributed to this industrial disaster, including money saving decisions that cut corners on safety, the decision to use a blowout preventer without adequately taking into account reported situations in which this mechanism could fail, incorrectly disregarding pressure test readings as anomalous, inadequate inspection practices, flawed cementing jobs, and insufficient regulatory oversight.[415] Though not directly located on the Gulf of Mexico, Oklahoma and New Mexico are also key States for the oil and natural gas subsectors and have similar vulnerabilities to industrial disasters.[416]

(U) From 1998 to 2009, there were 22 terrorist attacks in the region.[417] Ten of the 22 attacks were bombing/explosion attacks, all taking place in either New Mexico or Texas.[418] With the importance of the energy sector to not only this region, but the nation as a whole, any threat to industry in the region may have cascading impacts.

(U) The Energy Sector is critical to the regional economy. Al-Qa'ida and other terrorist organizations with which it is affiliated remain interested in attacking the Energy Sector as it contains valuable economic targets.[419] For example, the FBI warned the Texas oil industry of potential attacks on energy infrastructure leading up to the November 2004 elections.[420] The significant presence of petrochemical assets in the region could also make attractive targets. The threat of terrorism creates significant risk for the region. Given the importance of commercial facilities and energy assets in these States, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Defense Industrial Base Sector, and Water Sector.[421]

(U) Risks to Federally Administered Region VII

(U) Region VII is composed of Iowa, Kansas, Missouri, and Nebraska. Risks to the Chemical Sector and Food and Agriculture Sector are of greatest concern in this region. Since 1998, FEMA has issued 91 Federal disaster declarations for the States within the region.[422] Severe storms, tornadoes, and flooding are the costliest natural hazards to the region, accounting for over 90 percent of the Federal funds issued for recovery and response efforts during this time.[423] The region's most common natural hazards are floods, severe storms, and tornadoes.[424,425] Eastern Missouri lies within the New Madrid Seismic Zone, where some of the largest earthquakes in North America have occurred historically.

(U)Tornadoes are a major threat to the region, especially Kansas and Nebraska, with all of these States in the top 11 in the Nation, in terms of number of tornadoes and resulting economic damage.[426] The May 2011 tornado that hit the city of Joplin, Missouri, has a preliminary estimated cost of $1 to $3 billion.[427] The tornado left at least 125 people dead and several hundred injured, making it the single deadliest tornado to strike the United States since modern tornado recordkeeping began in 1950.[428] With a $30 billion increase in inland storm insurance claims in the past three years and an already record year for tornadoes, the threat of severe storms and tornadoes appears to be increasing,[429] also increasing risk for the region.

(U//FOUO) Reducing risk to and ensuring resilience of the Food and Agriculture Sector in this region is critical to the Nation's economy. All of these States are among the top 10 agricultural producing States in the country[430] and are famous for being part of the American heartland. They are also all among the top 12 States in terms of agricultural exports.[431] Iowa, for example, leads the country in sales of corn, grains and oilseeds, pigs, and chickens for egg production.[432] Despite this production, the Food and Agriculture Sector is vulnerable to naturally occurring and manmade hazards.[433] Chemicals and infectious diseases could be intentionally introduced at various points in the supply chain found in the region and cause severe economic consequences since the Food and Agriculture Sector accounts for about 13 percent of the gross domestic product and 18 percent of domestic employment in the United States.[434] Naturally occurring diseases also threaten the sector and could lead to disastrous consequences. An outbreak of food-and-mouth disease in the United Kingdom resulted in over $10 billion in losses to tourism and the Food and Agriculture Sector there.[435] A similar scenario in the United States could result in costs as high as $24 billion.[436] Threats and consequences have been and are expected to remain high for this sector, and these

along with current vulnerabilities, place this sector, the region, and the Nation at continued risk.

(U//FOUO)The Chemical Sector plays an important role in supporting the Food and Agriculture Sector in the region. For example, Dodge City, Kansas, has an important nitrogenous fertilizer plant,[437] and Hastings, Nebraska, has a distribution center for fertilizer.[438] Chemicals are also involved in the production process for Iowa's lucrative ethanol industry.[439] The Chemical Sector itself is also an integral component of the U.S. economy.[440] The terrorist threat to assets with the purpose of creating harmful public health and safety, [441] as well as economic[442] consequences, is of great concern and contributes to the region's risk.

(U) From 1998 to 2009, there were 17 terrorist attacks in the region.[443] Twelve of these were bombing/explosion attacks, and all 17 were directed against private citizens and property.[444] The threat of terrorism creates significant risk for the region. Given the importance of food, agriculture, and the chemical industry in these States and the dependence of the Food and Agriculture Sector on the Chemical Sector, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Defense Industrial Base Sector, and Food and Agriculture Sector.[445]

(U) Risks to Federally Administered Region VIII

(U) Region VIII is composed of Colorado, Montana, North Dakota, South Dakota, Utah, and Wyoming. Risks to the Dams Sector and the Water Sector are of greatest concern in this region. Since 1998, FEMA has issued 61 Federal disaster declarations for the States within the region.[446] The vast majority of these declarations were for disasters in North Dakota and South Dakota.[447] Severe storms and floods are the two costliest natural hazards to the region,[448] accounting for approximately 90 percent of the Federal funds issued for recovery and response efforts during this time.[449] The region's most common natural hazards are severe storms and events that cause flooding, flash flooding, and landslides.[450]

(U) The ongoing threat of severe storms and flooding contribute to regional risk. Montana and Wyoming frequently deal with the threat of floods from high snowpack levels in the Northern Rocky Mountains.[451] Further east, the Red River in North Dakota is very vulnerable to flooding and has exceeded flood stage in 47 of the past 108 years and every year from 1993 through 2010.[452] Severe winter storms in 2011 were major contributors to flooding, with the water content of the snowpack ranked among the highest in the last 60 years.[453] While the average annual flood damages from the Red River are estimated at more than $193 million, a 500-year event would flood nearly the entire city of Fargo with considerably higher economic costs.[454] Sections of the Red River at East Grand Forks peaked at more than 6.6 meters above flood stage in 1997, slightly exceeding the 500-year statistical recurrence interval at that site.[455] Though it is unknown when such an event would occur in Fargo, the city will remain at risk until a new floodwall or water diversion system is constructed to reduce this vulnerability.[456]

(U) Colorado hosts a large system of 1900 dams that is critical to providing water to its citizens. However, many of these dams are in need of repairs. Though rare, the threat of a major dam failure is a concern throughout the region. The last major dam failure in Colorado happened in 1982 when the earthen Lawn Lake Dam led to a breach that released 220 million gallons of water, killing three people and causing $31 million in damage around the town of Estes Park.[457] The failure of one or more of the Horsetooth Dams (part of the Big-Thompson water project, the largest trans-mountain water diversion project in Colorado) also could potentially inundate the Fort Collins, Colorado, area with property damage approaching $6 billion and affecting approximately 50,000 people.[458] The terrorist threat to Colorado dams was brought to light with the arrest of Khalid Aldawasari, who listed reservoir dams in Colorado as potential targets.[459] Ongoing threats to, and vulnerabilities within, the Dams Sector, as well as associated large-scale consequences, contribute to regional risk.

(U) The Water Sector provides drinking water for the large urban areas of Denver and Salt Lake City, generates electricity, and supports agriculture throughout the region. For example, the Colorado Big Thompson Water project serves all three of these purposes. As the system's water is pumped across the Continental Divide, it is used to generate electricity at five power plants, fill reservoirs used for drinking water, and irrigate 693,000 acres of Colorado farmland.[460] The Central Valley Water Reclamation Facility in Utah also treats 75 million gallons of waste water each day and serves over 500,000 people in the Salt Lake County.[461] As the region is prone to both droughts and floods, mitigation of the risk to this sector in the region is critical.

(U) From 1998 to 2009, there were 13 terrorist attacks in the region.[462] Six of these were facility/infrastructure attacks.[463] The region contains a significant number of National monuments and icons that could provide attractive targets. The threat of terrorism creates significant risk for the region. Given the importance of dams and water to these States, and the interdependence of the Dams Sector and the Water Sector, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Dams Sector, Defense Industrial Base Sector, and Food and Agriculture Sector.[464]

(U) Risks to Federally Administered Region IX

(U) Region IX is composed of Arizona, California, Hawaii, and Nevada, as well as the territories of American Samoa and Guam, the Commonwealth of the Northern Mariana Islands, the Republic of the Marshall Islands, and the Federated States of Micronesia.[465] Risks to the Commercial Facilities Sector and the Transportation Systems Sector are of greatest concern in the region. Since 1998, FEMA has issued 58 Federal disaster declarations for the States and territories within the region.[466] Severe storms are the costliest natural hazards to the region, accounting for nearly half the Federal disaster funds issued for recovery and mitigation in the region during this time.[rr,467] Fires account for almost 30 percent, and typhoons and earthquakes make up another 10 percent each.[468] The region's most common natural hazards are earthquakes, severe storms, typhoons, and wildfires. Tsunamis are a less frequent by still hazardous threat to coastal regions.[ss]

(U) The geology of the region, with some of the most active fault lines in the country,[469] makes the region particularly vulnerable to seismic events like earthquakes. For example, an earthquake with a 6.7 magnitude or larger has more than a 99 percent chance of occurring in California in the next 30 years.[470] Earthquakes could cause significant damage to critical infrastructure in the region,[471] especially with major fault lines located near the large urban centers of Los Angeles, San Diego, and San Francisco.[472] The magnitude 6.9 Loma Prieta earthquake that struck San Francisco in 1989 resulted in approximately $6 billion in economic costs.[473] An earthquake impacting the ports of Los Angeles and Long Beach also could be very expensive, as closing the ports for one week could cost $423 million to $1.5 billion.[474] Earthquakes also affect other States and territories in the region, with Hawaii experiencing earthquakes frequently. This ongoing threat and related vulnerabilities, as well as the potential for large and pervasive consequences, contribute to regional risk.

(U) Assets within the Commercial Facilities Sector are important drivers for the economy[475] and are at greater risk. Assets in this sector are highly visible, are easily accessible, have the potential to result in mass casualties if attacked or otherwise destroyed,[476] are symbolically important (as at theme parks[477]), and are of interest to terrorists, having been attacked previously. Open access counters the deterrence provided by security barriers at these facilities, making the sector more vulnerable to

[rr] (U) Severe storms that can produce heavy snows, flooding, high winds and even tornadoes are the most common weather threats in late winter and early spring. [Federal Emergency Management Agency, "Severe Weather Awareness Week," 8 March 2001]
[ss] (U) For example, the tsunami generated by the 8.9 magnitude Japanese earthquake on March 11, 2011 caused significant damage to Hawaii and northern California.

attacks[478] and increasing risk for the sector in the region. Events featuring mass gatherings that take over large areas of land and become small cities, such as NASCAR races in Arizona, California, and Nevada, possess unique vulnerabilities that create risk.[479] Terrorist attacks on commercial facilities in the region have been attempted in the past, including the thwarted al-Qa'ida/Jemaah Islamiyah plot to attack the U.S. Bank Tower in Los Angeles in 2003.[480] Resort hotels in Hawaii, gaming facilities in Nevada, major spring training facilities in Arizona, and entertainment production facilities in California are only a few examples of high-value commercial facilities in the region.[tt] Due to the visibility and economic value of some of these assets, the threat to commercial facilities in the region remains high, contributing greatly to regional risk.[481]

(U//FOUO) The Transportation Systems Sector is critical to the region due in large part to the geographic isolation of Hawaii and the island territories (American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, the Republic of the Marshall Islands, and the Federated States of Micronesia). Risks to this sector also affect the other sectors that depend upon it or with which it is interdependent.[482] For example, after the 1992 landfall of Hurricane Iniki in Hawaii (which caused $5 billion in damage),[483] recovery and restoration efforts in a number of other critical infrastructure sectors were hampered because airports and docks were damaged on the island of Kauai.[484] The region's transportation networks also have been targeted by terrorist groups in the past, such as with the 2000 Millennium Bomb Plot against Los Angeles International Airport.[485] Aviation assets remain top terrorist targets.[486] The region's urban areas, with 5 major metropolitan statistical areas ranked in the top 16 in the United States in terms of population size,[487] ensure that reliance on other critical infrastructure sectors, such as the Energy Sector, Food and Agriculture Sector, and Water Sector, will continue to grow in the coming years.

(U) From 1998 to 2009, there were 38 terrorist attacks in the region.[488] Thirteen were facility/infrastructure attacks, and 35 took place in California.[489] The terrorist threat to dams was also brought to light with the arrest of Khalid Aldawasari, who listed reservoir dams in California as potential targets.[490]As of February 2010, al-Qa'ida had identified Los Angeles among a number of important cities where attacks should occur. The symbolic value of Las Vegas and Reno as major cities with economies driven by the thriving gaming industry makes them high-value targets and creates greater risk for the Commercial Facilities Sector within the region. Icons such as the Hoover Dam also make high-value targets. The threat of terrorism creates significant risk for the region. Given the importance of commercial facilities and transportation in these States, and the

[tt] (U) In 2010, Las Vegas/Clark County attracted 37 million visitors, 18,000 conventions and trade shows, and gaming revenue of $8.9 billion. [*Las Vegas Convention and Visitors Authority*, Frequently Asked Questions, www.lvcva.com/press/statistics-facts/visitor-stats.jsp, accessed 9 May 2011]

interdependence of the Commercial Facilities Sector and the Transportation Systems Sector, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk due to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Commercial Facilities Sector, Dams Sector, Defense Industrial Base Sector, Food and Agriculture Sector, Transportation Systems Sector, and Water Sector.[491]

(U) Risks to Federally Administered Region X

(U) Region X is composed of Alaska, Idaho, Oregon, and Washington. Risks to the Energy Sector and Transportation Systems Sector are of greatest concern in this region. Since 1998, FEMA has issued 43 disaster declarations for the States within the region, with 29 of these directly linked to damage caused by severe storms.[492] Severe storms and earthquakes are the two costliest natural hazards to the region,[493] with severe storms accounting for approximately 65 percent of Federal funds issued for recovery and response efforts in the region during this time.[494] The region's most common natural hazards are earthquakes, landslides, severe storms and flooding, tornadoes, volcanic eruptions, and wildfires.[495] Tsunamis are a less frequent by still hazardous threat to coastal regions.[uu]

(U) Earthquakes are common in the region, with more earthquakes occurring in Alaska than in all other States combined.[496] The 1964 Alaska 9.2 magnitude earthquake, the largest recorded in U.S. history,[497] caused 128 deaths and about $311 million in property loss.[498] The coastal areas of Oregon and Washington also lie at a convergent continental margin where the Cascadia subduction zone and the Juan de Fuca plates meet, increasing the potential for seismic activity.[499] The region's most populous city, Seattle, remains vulnerable to earthquakes because it sits atop a sedimentary basin that strongly affects the patterns of earthquake ground shaking and, therefore, potential damage.[500]

(U//FOUO) The Transportation Systems Sector is critical to the region. Alaska's geographical separation from the rest of the region and the continental United States highlights the importance of the region's transportation infrastructure for both daily activities and emergency response.[501] Alaska relies on ports in Washington State, which possesses the largest locally controlled public port system in the world, handling approximately seven percent of all U.S. exports and six percent of all U.S. imports. Together, the Ports of Seattle and Tacoma, Washington, make up the second-largest container complex in the United States,[502] while the Washington State Ferry System is the largest ferry transit system in the country, incorporating both ports of entry and border crossings with Canada.[503] International terrorist groups have attacked maritime assets around the world, and threats to these assets create additional regional risk.[504]

(U) Interdependencies of the Energy Sector with other sectors in the region are very important. Alaska ranks second in the Nation for crude oil production, with the Prudhoe

[uu] (U) Although the tsunami generated by the 8.9 magnitude Japanese earthquake on March 11, 2011 did not cause massage damage regionally, the Port of Brookings Harbor, Oregon, sustained heavy damage.

Bay on Alaska's North Slope producing approximately 264,000 barrels per day as the highest yielding oil field in the United States.[505] The Trans-Alaska Pipeline, another critically important piece of the Nation's transportation infrastructure (one that is challenging to protect for many reasons, such as its length and remote location[506]), transports crude oil from the North Slope to the Port of Valdez in southern Alaska, where it is shipped to refineries in Washington before heading to Portland, Oregon, and the rest of the region via the Olympic pipeline.[507] Once refined, approximately 26,000 barrels of oil[508] travel on barges via the Columbia River to support the Food and Agriculture Sector and Transportation Systems Sector in Idaho, Oregon, and Washington.[509] The United States also shipped 10.4 million tons of wheat through the Pacific Northwest (about 40 percent of total exports) last year. Any disturbance in these interdependent sectors, such as fuel shortages or prolonged closure of locks and dams on the Columbia River, could have significant economic impact[510] and place the Energy Sector, as well as the region, at greater risk.

(U) Terrorist attacks have also occurred in the region. From 1998 to 2009, there were 23 terrorist attacks in the region.[511] Fifteen were facility/infrastructure attacks, half of which were directed at businesses.[512] Seattle, Washington is also a potential target for international terrorists. Khalid Sheikh Mohammad, the mastermind of the September 11, 2001 attacks put the Northwest's tallest building on his top 10 target list. Later, U.S. forces found photographs of the Space Needle in an al-Qa'ida hideout in Afghanistan. The threat of terrorism creates significant risk in the region. Given the importance of energy and transportation in these States, and the dependence of the Transportation Systems Sector on the Energy Sector, the threat of a terrorist attack on either or both of these sectors creates even greater risk to the region.

(U//FOUO) Analysis of nationally significant critical infrastructure in the region indicates that the following sectors are at risk owing to their significant physical presence and the potential for greater consequences if they are attacked or fail: the Chemical Sector, Commercial Facilities Sector, Dams Sector, Energy Sector, and Transportation Systems Sector.[513]

(U) Conclusion: Path Forward to the Next National Risk Profile

(U) The 2011 National Risk Profile provides a baseline for ongoing and potential future risks to the critical infrastructure. Subsequent Profiles will use the 2011 National Risk Profile as their baseline and will address those aspects of critical infrastructure risk that have changed or for which our understanding has changed. When the National Risk Landscape changes drastically in the future, the baseline for the National Risk Profile will be reestablished.

(U) The next National Risk Profile will incorporate additional input from critical infrastructure stakeholders and partners as early as possible in the development process. First, the national cross-cutting, regional, and sectoral risks will be revisited with an eye towards identifying those areas where the risks have changed and/or understanding by members of the critical infrastructure community of those risks has changed.

(U) Thereafter and throughout the period of development for the National Risk Profile, a variety of inputs will be solicited. These include but are not limited to: verbal and written comments from critical infrastructure members and experts, as well as data generated by critical infrastructure sectors, studies conducted by the National Laboratories, and perspectives from homeland security leaders throughout the public and private sector.

(U) Information will also be gathered through site visits to the ten federally administered regions. Federal and non-federal personnel that are responsible for regional risk mitigation will be asked to provide their input and guide those responsible for developing the National Risk Profile to observe the impact of those national cross-cutting, regional, and sectoral risks that they feel affect their own regions.

(U) The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) provides our partners throughout the critical infrastructure and resilience communities with the information they need to manage the risks they face. The National Risk Profile is one way in which that information is provided. The National Risk Profile also helps these leaders to plan and allocate resources using risk-informed metrics—a top priority of the Department of Homeland Security Office of Infrastructure Protection Critical Infrastructure Risk Management Enhancement Initiative.

(U) The National Risk Profile helps risk managers understand the critical infrastructure risks they face now and may face in the future, as well as the context in which those risks play out. With the National Risk Profile, we hope our critical infrastructure and resilience leaders can better address the risks of tomorrow with the leadership and resources of today.

(U) Definitions[vv]

(U) Consequence	The effect of an event, incident or occurrence. Consequence is commonly measured in four ways (human, economic, mission, and psychological) but may also include other factors, such as impact on the environment.
(U) Dependency	The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction or other requirement from other sources in order to function properly.
(U) Interdependency	The mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.
(U) Risk	The potential for an unwanted outcome resulting from an incident, event or occurrence, as determined by its likelihood and the associated consequences. The potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.
(U) Threat	A natural or manmade occurrence, individual, entity or action that has harmed or has indicated the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an intentionally-introduced hazard is generally estimated as the likelihood of an attack being attempted by an adversary.
(U) Vulnerability	The probability of an attack, once launched, that will succeed in destroying, disabling, or otherwise significantly harming the target or system.

[vv] (U) For additional definitions, see the DHS Risk Lexicon.

(U) Endnotes

[1] (U) U.S. Geological Survey, *Natural Hazards – A National Threat*, Washington, DC: U.S. Department of the Interior, 2007, pubs.usgs.gov/fs/2007/3009, accessed April 7, 2011.
[2] (U) Kappenman JG, Zanetti, LJ, and Radasky, WA, *Geomagnetic Storms Can Threaten Electric Power Grid*, EV World, accessed at http://evworld.com/article.cfm?storyid=246 on April 22, 2011.
[3] (U) Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, *Severe Space Weather Events – Understanding Societal and Economic Impacts: a workshop report*, Washington, DC: National Academies Press, 2008: p. 22, www.nap.edu/catalog/12507.html, accessed 31 March 2011.
[4] (U) National Aeronautics and Space Administration, *Deep Solar Minimum*, science.nasa.gov/science-news/science-at-nasa/2009/01apr_deepsolarminimum/, accessed April 25, 2011.
[5] (U) National Aeronautics and Space Administration, *Solar Activity Heats Up,* science.nasa.gov/science-news/science-at-nasa/2011/14apr_thewatchedpot/*,* accessed April 25, 2011.
[6] (U) Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, *Severe Space Weather Events – Understanding Societal and Economic Impacts: a workshop report*, Washington, DC: National Academies Press, 2008: p. 22, www.nap.edu/catalog/12507.html, accessed 31 March 2011.
[7] (U) Committee on the Societal and Economic Impacts of Severe Space Weather Events, Space Studies Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, *Severe Space Weather Events – Understanding Societal and Economic Impacts: a workshop report*, Washington, DC: National Academies Press, 2008: p. 16, www.nap.edu/catalog/12507.html, accessed March 31, 2011.
[8] (U) Moran, A, "NASA Views Extraordinary Coronal Mass Ejection, Solar Flares," *Helium News* (June 8, 2010), accessed at http://news.helium.com/news/13534-nasa-views-extraordinary-coronal-mass-ejection-solar-flares, on June 18, 2011.
[9] (U) Riccardi, N., "Chevron Told to Close Pipeline After Second Oil Spill in Salt Lake City," Los Angeles Times (December 10, 2010), articles.latimes.com/2010/dec/10/nation/la-na-utah-oil-spill-20101211, accessed March 31, 2011.
[10] (U) Federal Emergency Management Agency, *Backgrounder: Extreme Heat*, www.fema.gov/hazard/heat/background.shtm, accessed March 31, 2011.
[11] (U) UN-Habitat, *Urbanization: Facts and Figures*, accessed at www.unhabitat.org/mediacentre/documents/backgrounder5.doc on June 19, 2011.
[12] (U) Federal Emergency Management Agency, *Declared Disasters and Emergencies,* www.fema.gov/news/disasters.fema, accessed June 25, 2011.
[13] (U) Federal Emergency Management Agency, *Declared Disasters by Year or State*, www.fema.gov/news/disaster_totals_annual.fema, accessed June 25, 2011.
[14] (U) Munich Re Group, *Topics Geo Natural Catastrophes 2008: analyses, assessments, positions*, Munchen, Germany: Munchener Ruckversicherungs-Gesellschaft, 2009, www.preventionweb.net/files/13201_topics2008.pdf?bcsi_scan_1CFAD6D3D20A37D6=0&bcsi_scan_filename=13201_topics2008.pdf, accessed March 30, 2011.
[15] (U) McWhirter, C., "Extreme Drought Grips Parts of South, Midwest," *The Wall Street Journal* (October 20, 2010), online.wsj.com/article/SB10001424052702304011604575564520488798994.html, accessed March 31, 2011.
[16] (U) World Health Organization, *Pandemic Preparedness: consequences of an influenza pandemic*, accessed at http://www.who.int/csr/disease/influenza/pandemic/en/ on May 10, 2011.
[17] (U) American Public Health Association, *Get the Facts: Pandemic Flu*, p. 1, accessed at http://www.apha.org/NR/rdonlyres/A12756DD-5FB1-4CDD-8746-C9F3B1099686/0/PandemicFlu.pdf on May 10, 2011.
[18] (U) World Health Organization, *Pandemic Preparedness: consequences of an influenza pandemic,* accessed at http://www.who.int/csr/disease/influenza/pandemic/en/ on May 10, 2011.
[19] (U) American Public Health Association, *Get the Facts: Pandemic Flu*, p. 1, accessed at http://www.apha.org/NR/rdonlyres/A12756DD-5FB1-4CDD-8746-C9F3B1099686/0/PandemicFlu.pdf on May 10, 2011.
[20] (U) Majority Staff, Committee on Homeland Security, *Getting Beyond Getting Ready for Pandemic Influenza*, Washington, DC: US House of Representatives, June 2009, p. 20, accessed at http://chsdemocrats.house.gov/SiteDocuments/20090114124322-85263.pdfon May 10, 2011.
[21] (U) National Infrastructure Simulation and Analysis Center, *National Population, Economic, and Infrastructure Impacts of Pandemic Influenza with Strategic Recommendations*, Washington, DC: Department of Homeland Security, October 2007, p. 56.
[22] (U) Ibid, p. 52-53.
[23] (U) Ibid, p. 41-46.
[24] (U) Ibid, p. 39-41.
[25] (U) Ibid, p. 47-50.
[26] (U) Ibid, p. 41-46.
[27] (U) Ibid, p. 46.
[28] (U) Ibid, p. 39-41.
[29] (U) http://hpsweb.honeywell.com/Cultures/en-US/AboutUs/PartnershipsAlliances/AbnormalSituationManagement/default.htm.
[30] (U) U.S. Department of Transportation, Federal Highway Administration, Structures, Structure Type by Year Built, As of December 2008.
[31] (U) America 2050, "An Infrastructure Vision for 21 Century America", p.4.

PLANYC Website, http://www.nyc.gov/html/planyc2030/html/challenge/maintainyc.shtml (accessed on September 14, 2009).
[32] (U) National Council on Public Works Improvement, "Fragile Foundations: A Report on America's Public Works", Final Report to the President and Congress, February 1988. See also: American Society of Civil Engineers, Report Card for America's Infrastructure, http://www.infrastructurereportcard.org/index.
[33] (U) Lewis, Richard O., Report of Findings, Forensic Investigation of 66-Inch PCCP Water Transmission Main Failure on December 23, 2008, 8500 River Road, Bethesda, Montgomery County, MD, Conducted for Washington Suburban Sanitary Commission; Lewis Engineering and Consulting. Inc., Gainesville, FL; pp. 20-21.
[34] (U) National IPR Coordination Center, *Fact Sheet: Operation Guardian,* Washington, DC: US Immigration and Customs Enforcement, ice.gov/news/library/factsheets/guardian.htm, accessed April 26, 2011. See also: Progressive Policy Institute, *Worldwide Market for Counterfeit Goods: $650 billion*, http://www.ppionline.org/ppi_ci.cfm?knlgareaid=108&subsecid=900003&contentid=253907, accessed April 26, 2011.
[35] (U) American Society of Civil Engineers (ASCE), *2009 Report Card for America's Infrastructure*, Reston, VA: American Society of Civil Engineers, 2009, accessed at www.infrastructurereportcard.org/report-cards, accessed April 26, 2011.
[36] (U) National Transportation Safety Board, Pipeline Accident Report, "Natural Gas Pipeline Rupture and Fire Near Carlsbad, New Mexico, August 19, 2000, NTSB/PAR-03/01, at p. 49.
[37] (U) http://www.businesswire.com/news/home/20101202005750/en/Research-Markets-Utilities-Technology---2011-Trends. Radice SA, *The Dual Threat: Aging Infrastructure and Aging Workforce Call for Integrated Asset Management and Workforce Management,* Ventyx, 2008, www1.ventyx.com/pdf/wp08-the-dual-threat.pdf, accessed April 26, 2011.
[38] (U) For example, the National Infrastructure Simulation and Analysis Center (NISAC) has identified a variety of sectors that could face significant age-related challenges in the future due to a large proportion of sector assets requiring replacement at the same time.
[39] (U) http://www.cutter.com/content/trends/fulltext/advisor/2011/btt110317.html
[40] (U) http://www.infrastructurist.com/2011/03/02/top-world-bank-economist-us-should-invest-in-infrastructure/
[41] (U) http://www.oliverwyman.com/.../Energy06-Aging_Infrastructure.pdf
[42] (U) http://www.infrastructurist.com/2011/02/22/the-2011-infrastructurist-forum-part-ii/
[43] (U) http://www.businessdictionary.com/definition/municipal-bond.html; www.etftrends.com/2010/12/coming-america-infrastructure-etfs/, accessed on May 25, 2011.
[44] (U//FOUO) DHS Office of Intelligence and Analysis, Update: Homeland Security Threat Assessment: Evaluating Threats 2009-2014, 5 May 2011.
[45] (U//FOUO) DHS Office of Intelligence and Analysis, Evolution of the Terrorist Threat to the United States, 21 May 2010.
[46] (U) National Intelligence Estimate: The Terrorist Threat to the US Homeland, July 2007.
[47] (U) Homeland Infrastructure Threat and Risk Assessment Center, *(U) Infrastructure Protection Note: Preparing for an Evolving Terrorist Threat*, Office of Infrastructure Protection, Department of Homeland Security, May 26, 2010, p.2.
[48] (U//FOUO) DHS Office of Intelligence and Analysis, February 2010 Al-Qa'ida Homeland Plotting Priorities Included Symbolic Dates and Major U.S. Cities, 20 May 2011.
[49] (U) Homeland Infrastructure Threat and Risk Assessment Center, *(U) Infrastructure Protection Note: Preparing for an Evolving Terrorist Threat*, Office of Infrastructure Protection, Department of Homeland Security, May 26, 2010, p. 2.
[50] (U) Napolitano J., Testimony of Secretary of Homeland Security Janet Napolitano before the Senate Committee on the Judiciary, Hearing on "Department of Homeland Security Oversight," 112th Congress, 1st session, March 9, 2011, www.dhs.gov/ynews/testimony/testimony_1299683039975.shtm, accessed March 31, 2011.
[51] (U) Johnson, K, "Officials Warn of Domestic Terrorism Threat," *Wall Street Journal,* February 10, 2011, accessed at http://online.wsj.com/article/SB10001424052748703716904576134373186541808.html on June 19, 2011.
[52] (U) Ibid.
[53] (U) Homeland Infrastructure Threat and Risk Assessment Center, *(U) Infrastructure Protection Note: Preparing for an Evolving Terrorist Threat*, Office of Infrastructure Protection, Department of Homeland Security, May 26, 2010, p. 1.
[54] Ibid.
[55] (U//FOUO) DHS Office of Intelligence and Analysis, AQAP Releases Special Issue of *Inspire* Highlighting Recently Disrupted Parcel Bomb Plot, 21 November 2011.
[56] (U) Lake, Jennifer E., *Border Security: the complexity of the challenge,* Congressional Research Service: Washington, DC, January 24, 2007, p.2.
[57] (U) Immigration and Customs Enforcement, *"Worksite Enforcement – Critical Infrastructure Protection*, accessed at: http://www.ice.gov/worksite/ on May 23, 2011.
[58] (U) Immigration and Customs Enforcement, *"DMV examiners and customers charged with document fraud: 18 individuals charged in scheme, including four Department of Motor Vehicles employees,"* accessed at http://www.ice.gov/news/releases/1105/110502miami.htm on May 23, 2011.
[59] (U) Mortensen, Ronald W., *Illegal But Not Undocumented: Identify Theft, Document Fraud, and Illegal Employment*, Center for Immigration Studies, accessed at: http://www.cis.org/identitytheft on May 23, 2011.
[60] (U) Ibid.
[61] (U) Ibid.
[62] (U) Immigration and Customs Enforcement, *Fact Sheet: Operation Guardian*, accessed at http://www.ice.gov/news/library/factsheets/guardian.htm on May 23, 2011.
[63] (U) Customs and Border Protection, *CBP, ICE Release Report on 2010 Counterfeit Seizures*, accessed at: http://www.cbp.gov/xp/cgov/newsroom/news_releases/national/03162011.xml on May 23, 2011.
[64] (U) Customs and Border Protection and Immigration and Customs Enforcement, *Intellectual Property Rights: Fiscal Year 2010 Seizure Statistics – Final Report,* p. 7, accessed at http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/seizure/seizure_stats_fy2010.ctt/seizure_stats_fy2010.pdf on May 23, 2011.

[65] (U) Immigration and Customs Enforcement, *Fact Sheet: Operation Guardian*, accessed at http://www.ice.gov/news/library/factsheets/guardian.htm on May 23, 2011.
[66] (U) Customs and Border Protection and Immigration and Customs Enforcement, *Intellectual Property Rights: Fiscal Year 2010 Seizure Statistics – Final Report,* p. 14, accessed at http://www.cbp.gov/linkhandler/cgov/trade/priority_trade/ipr/pubs/seizure/seizure_stats_fy2010.ctt/seizure_stats_fy2010.pdf on May 23, 2011.
[67] (U) Immigration and Customs Enforcement, *Fact Sheet: Operation Guardian*, accessed at http://www.ice.gov/news/library/factsheets/guardian.htm on May 23, 2011.
[68] (U) Immigration and Customs Enforcement, *Fact Sheet: Operation Firewall*, accessed at http://www.ice.gov/news/library/factsheets/firewall.htm on May 23, 2011.
[69] (U) Homeland Security Newswire, March 27, 2006, Analysis: Even if chemical plants are more secure, transportation of chemicals will not be, accessed at http://homelandsecuritynewswire.com/analysis-even-if-chemical-plants-are-more-secure-transportation-chemicals-will-not-be on May 23, 2011.
[70] (U) Brandon, J, *GPS Jammers Illegal, Dangerous, and Very Easy to* Buy, FOXNews, March 17, 2010, http://www.foxnews.com/scitech/2010/03/17/gps-jammers-easily-accessible-potentially-dangerous-risk/, accessed May 11, 2011.
[71] (U) Immigration and Customs Enforcement, *Fact Sheet: Operation Guardian*, accessed at http://www.ice.gov/news/library/factsheets/guardian.htm on May 23, 2011.
[72] (U) US-Canada Power System Outage Task Force, accessed at https://reports.energy.gov/ on May 23, 2011.
[73] (U) Harding, Anne, US Borders at Risk of Bio-invaders, *The Scientist*, May 16, 2007, accessed at http://www.the-scientist.com/news/display/53195/ on May 23, 2011.
[74] (U) Wolf, Aaron T. and Newton, Joshua T., *Case Study of Transboundary Dispute Resolution: U.S./Mexico shared aquifers,* accessed at http://www.transboundarywaters.orst.edu/research/case_studies/US_Mexico_Aquifer_New.htm on May 23, 2011.
[75] (U) M86 Security Labs, *Security Labs Report, January - June 2010*, http://www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_1H2010.pdf, accessed 10 May 10, 2011.
[76] (U) SANS (SysAdmin, Audit, Network, Security) Institute, "Top Cyber Security Risks," September 2009, www.sans.org/top-cyber-security-risks/summary.php, accessed March 31, 2011.
[77] (U) Lynn, William J. III, Remarks on Cyber at the RSA Conference, San Francisco, California, Tuesday, February 15, 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1535, accessed May 15, 2011.
[78] (U) Analysis from the Department of Homeland Security, National Cyber Security Division, Critical Infrastructure Protection Cyber Security (CIP CS) Program, April 2011.
[79] (U) SANS Institute, *The Top Cyber Security Risks*, September 2009, http://www.sans.org/top-cyber-security-risks/summary.php, accessed June, 27, 2010.
[80] (U) National Cyber Security Alliance/ Symantec/ Zogby, *2009 National Cyber Security Alliance/ Symantec Home User Study*, October 2009, pp. 5-7, http://www.staysafeonline.org/sites/default/files/resource_documents/Home%20User%20Study%20FINAL.pdf, accessed May 11, 2011.
[81] (U) White House, *Cyberspace Policy Review*, May 2009, p. 33.
[82] (U) National Security Council and the Homeland Security Council, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington, DC, The White House, 2009: p. 2, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, accessed March 31, 2011.
[83] (U) National Intelligence Council, *Global Trends 2025: a Transformed World*, Washington, DC: Director of National Intelligence, 2008: p. 97, www.dni.gov/nic_2025_project.html, accessed March 31, 2011.
[84] (U) http://www.911dispatch.com/info/cad/index.html, accessed May 11, 2011.
[85] (U) Brandon, J, *GPS Jammers Illegal, Dangerous, and Very Easy to* Buy, FOXNews, March 17, 2010, http://www.foxnews.com/scitech/2010/03/17/gps-jammers-easily-accessible-potentially-dangerous-risk/, accessed May 11, 2011.
[86] (U) Higgins, KJ, *Encrypted GSM Voice Calls and SMS Messages Hacked in Minutes*, Dark Reading, http://www.darkreading.com/security/encryption/211201467/index.html, accessed May 11, 2011.
[87] (U) Department of Homeland Security and Department of the Treasury, "Banking and Finance: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, May 2007, http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf, accessed May 9, 2011.
[88] (U) Ibid.
[89] (U) Department of Homeland Security, "Banking and Finance Sector Snapshot," 2010.
[90] (U) Government Accountability Office, "Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Grow, Committee on Financial Services, House of Representatives: Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats," January 2003, http://www.gao.gov/new.items/d03173.pdf , accessed May 10, 2011.
[91] (U) Ibid.
[92] (U) 2010 Data Breach Investigations Report (A Study Conducted by the Verizon RISK Team in cooperation with the United States Secret Service, July 2010, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf, accessed May 13, 2011.
[93] (U) Government Accountability Office, "Report to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Grow, Committee on Financial Services, House of Representatives: Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats," January 2003, http://www.gao.gov/new.items/d03173.pdf , accessed May 10, 2011.
[94] (U) Ibid.
[95] (U) Ibid.
[96] (U) *2010 Data Breach Investigations Report* (A Study Conducted by the Verizon RISK Team in cooperation with the United States Secret Service), July 2010, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf, accessed May 13, 2011.

[97] (U) Congressional Research Service, *Banking and Financial Infrastructure Continuity: Pandemic Flu, Terrorism, and Other Challenges*," May 4, 2009, http://www.fas.org/sgp/crs/misc/RL31873.pdf, accessed May 13, 2011.
[98] (U) Ibid.
[99] (U) Ibid.
[100] (U) Ibid.
[101] (U) Ibid.
[102] (U) Ibid.
[103] (U) Department of Homeland Security, "Banking and Finance Sector Snapshot," 2010.
[104] (U) Ibid.
[105] (U) Ibid.
[106] (U) Department of Homeland Security, "Critical Infrastructure and Key Resources: Commercial Facilities Sector," http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/comFac1.htm, accessed June 20, 2011.
[107] (U) Ibid.
[108] (U) Department of Homeland Security, *Chemical Sector: Critical Infrastructure and Key Resources*, http://www.dhs.gov/files/programs/gc_1188567509125.shtm, accessed on May 6 2011.
[109] (U) *BBC*, "1984: Hundreds die in Bhopal chemical accident," http://news.bbc.co.uk/onthisday/hi/dates/stories/december/3/newsid_2698000/2698709.stm, accessed on May 31, 2011. The Bhopal incident was not the result of an intentional act, but it illustrates the potential consequences of industrial systems failures within the Chemical Sector.
[110] (U) Broad, William J., Markoff, John, and Sanger, David E., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *The New York Times*, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2, accessed on May 31, 2011.
[111] (U) *Federal Register*, "National Protection and Programs Directorate; Chemical Facility Anti-Terrorism Standards Personnel Surety Program," http://www.federalregister.gov/articles/2010/04/13/2010-8312/national-protection-and-programs-directorate-chemical-facility-anti-terrorism-standards-personnel#h-10, accessed on May 31, 2011.
[112] (U) Noonan, Thomas, and Archuleta, Edmund, "The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures," http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, accessed on May 31, 2011.
[113] (U) *BBC*, "Anger at Toulouse blast location," http://news.bbc.co.uk/2/hi/europe/1557644.stm, accessed on Jun 16, 2011. See also Fire and Blast Information Group (FABIG), http://www.fabig.com/NR/rdonlyres/BAE3F92B-9AE9-4697-BBC2-F6E1B0C4431D/2691/Toulouse.pdf, accessed on June 16, 2011.
[114] (U) U.S. Department of Labor, "Phillips 66 Company Houston Chemical Complex Explosion and Fire," April 1990, http://ncsp.tamu.edu/reports/phillips/first%20part.pdf, accessed June 20, 2011.
[115] (U) Department of Homeland Security, *Chemical Sector-Specific Plan*, 2010, http://www.dhs.gov/xlibrary/assets/nipp-ssp-chemical-2010.pdf, accessed June 9, 2011.
[116] (U) Department of Homeland Security, *Commercial Facilities Sector: Critical Infrastructure and Key Resources*, www.dhs.gov/files/programs/gc_1189101907729.shtm, accessed on May 13, 2011.
[117] (U) House Committee on Homeland Security, Majority Staff Report Examining: "Public Health, Safety, and Security for Mass Gatherings," May 2008, https://hsdl.org/?view&doc=95328&coll=limited, accessed on June 14, 2011.
[118] (U) Mueller, Robert S., Federal Bureau of Investigation, "Statement Before the Senate Committee on Appropriations," April 15, 2010, www2.fbi.gov/congress/congress10/mueller041510.htm, accessed May 13, 2011.
[119] (U) Federal Bureau of Investigation, "First Strike: Global Terror in America," February 26, 2008, www.fbi.gov/news/stories/2008/february/tradebom_022608, accessed on June 14, 2011.
[120] (U) Federal Bureau of Investigation, Counterterrorism Threat Assessment and Warning Unit, 1996, "Terrorism in the United States: 1996," www.fbi.gov/stats-services/publications/terror_96.pdf, accessed on June 14, 2011.
[121] (U) Federal Bureau of Investigation, "The Times Square Case," May 4, 2010, www.fbi.gov/news/stories/2010/may/timessquare_050410/times-square-case, accessed on June 14, 2011.
[122] (U) Mueller, Robert S., Federal Bureau of Investigation, "Statement Before the Senate Committee on Appropriations," April 15, 2010, www2.fbi.gov/congress/congress10/mueller041510.htm, accessed May 13, 2011.
[123] (U) Department of Homeland Security, *Commercial Facilities Sector: Critical Infrastructure and Key Resources*, accessed at www.dhs.gov/files/programs/gc_1189101907729.shtm on May 13, 2011.
[124] (U) The Guardian, "Eight dead as bombers target Western-owned Jakarta hotels," July 17, 2009, www.guardian.co.uk/world/2009/jul/17/bombs-explode-hotels-indonesia, accessed June 14, 2011.
[125] (U) CNN, "Deadly blast targets Marriott Hotel in Islamabad," September 20, 2008, http://articles.cnn.com/2008-09-20/world/pakistan.islamabad.marriott.blast_1_vehicle-bomb-explosion-bodies?_s=PM:WORLD, accessed on June 14, 2011.
[126] (U) RAND, "The Lessons of Mumbai," 2009, assessed at www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf on June 14, 2011.
[127] (U) Bloomberg, "Jakarta Bombs Show Hotels Still Favored Terror Target," July 18, 2009, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aQAhI4rtQcpQ, accessed June 16, 2011.
[128] (U) Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism, www.start.umd.edu/gtd/search/Results.aspx?start_yearonly=&end_yearonly=&start_year=&start_month=&start_day=&end_year=&end_month=&end_day=&asmSelect0=&asmSelect1=&weapon=5&attack=2&target=1&target=14&target=15&target=18&dtp2=all&success=yes&casualties_type=b&casualties_max=, accessed May 13, 2011.
[129] (U) Simon, Steven and Jonathan Stevenson, "Al-Qaeda's new strategy: Less apocalypse, more street fighting," *The Washington Post,* October 10, 2010, www.washingtonpost.com/wp-dyn/content/article/2010/10/08/AR2010100802664.html, accessed May 13, 2011.
[130] (U) Ibid.

[131] (U) National Retail Federation, "NRF-ICSC Emergency Response Protocols to Active Shooters," 2008, www.lpinformation.com/Portals/0/NRF_ActiveShooter_Guidelines.pdf, accessed May 13, 2011.
[132] (U) Clapper, James R., Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence," February 10, 2011, assessed at www.dni.gov/testimonies/20110210_testimony_clapper.pdf on June 14, 2011.
[133] (U) Karam, P.A., "Radiological Terrorism," *Human and Ecological Risk Assessment*, 11:502-523, 2005.
[134] (U) National Research Council, *Radiation Source Use and Replacement,* Washington, Committee on Radiation Source Use and Replacement, National Academies Press, Washington, DC, 2008, www.nap.edu/catalog.php?record_id=11976, accessed May 2, 2011.
[135] (U) Central Intelligence Agency, "Terrorist CBRN: Materials and Effects," May 2003, www.cia.gov/library/reports/general-reports-1/terrorist_cbrn/terrorist_CBRN.htm, accessed May 13, 2011.
[136] (U) Department of Homeland Security, *Commercial Facilities Sector-Specific Plan*, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf, accessed May 13, 2011.
[137] (U) Department of Homeland Security, "Communications Sector Snapshot," www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf, accessed May 11, 2011.
[138] (U) Department of Homeland Security, *Communications Sector-Specific Plan*, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf, accessed June 21, 2011.
[139] (U) Kowalski, E. and D. Cappelli, U.S. Secret Service and Carnegie Mellon, "Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector," January 2008, www.cert.org/archive/pdf/insiderthreat_it2008.pdf, accessed May 11, 2011.
[140] (U) CENTRA Technology, on behalf of Department of Homeland Security, Office of Risk Management and Analysis, "OECD Futures Project on Future Global Shocks: Geomagnetic Storms," January 14, 2011, www.oecd.org/dataoecd/57/25/46891645.pdf?bcsi_scan_1CFAD6D3D20A37D6=bCHlqgmJmCJjVtZNG26itk7BN9QNAAAALuRmTw==&bcsi_scan_filename=46891645.pdf, accessed May 11, 2011.
[141] (U) National Security Telecommunications Advisory Committee (NSTAC), "NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System," February 28, 2008.
[142] (U) Department of Homeland Security, "Communications Sector Snapshot," www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf, accessed May 11, 2011.
[143] (U) Federal Communications Commission, "Communications Interdependencies," http://transition.fcc.gov/pshs/techtopics19.html, accessed June 10, 2011.
[144] (U) Department of Homeland Security, "Critical Manufacturing Sector Snapshot," www.dhs.gov/xlibrary/assets/nipp_snapshot_criticalmanufacturing.pdf, accessed June 20, 2011.
[145] (U) Ibid.
[146] (U) Stecke, Kathryn E. and Kumar, Sanjay, "Sources of Supply Chain Disruptions, Factors that Breed Vulnerability, and Mitigating Strategies," University of Texas at Dallas School of Management, April 2010.
[147] (U) Peck, H., Abley, J., Christopher, M., Haywood, M., Saw, R., Rutherford, C., and Strathern, M., "Creating Resilient Supply Chains: A Practical Guide," Centre for Logistics and Supply Chain Management, Cranfield School of Management, Cranfield, UK (2003).
[148] (U) Ibid.
[149] (U) Haveman, Jon D. and Howard J. Shatz, eds., *Protecting the Nation's Seaports: Balancing Security and Cost*, San Francisco: Public Policy Institute of California, 2006.
[150] (U) Kawamoto, Dawn, "Port Closures Hamper Tech Shipments," CNET News Online, http://news.cnet.com/Port-closures-hamper-tech-shipments/2100-1005_3-960224.html, accessed May 3, 2011.
[151] (U) Stecke, Kathryn E. and Kumar, Sanjay, "Sources of Supply Chain Disruptions, Factors that Breed Vulnerability, and Mitigating Strategies," University of Texas at Dallas School of Management, April 2010.
[152] (U) Baker, Stewart, with Natalia Filipiak and Katrina Timlin, "In the Dark: Crucial Industries Confront Cyberattacks," McAfee second annual critical infrastructure report (written with the Center for Strategic and International Studies), 2011.
[153] (U) Ibid.
[154] (U) Homeland Security Newswire, "Stuxnet heralds age of cyber weapons, virtual arms race," http://homelandsecuritynewswire.com/stuxnet-heralds-age-cyber-weapons-virtual-arms-race, accessed May 3, 2011.
[155] (U) Keeney, M., Kowalski, E., Capelli, D., Moore, A., Shimeall, T., and Rogers, S., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," United States Secret Service and Carnegie Mellon CERT Software Engineering Institute, May 2005.
[156] (U) Ibid.
[157] (U) Stecke, Kathryn E. and Kumar, Sanjay, "Sources of Supply Chain Disruptions, Factors that Breed Vulnerability, and Mitigating Strategies," University of Texas at Dallas School of Management, April 2010.
[158] (U) Department of Homeland Security, *Dams Sector-Specific Plan*, 2010.
[159] (U) Department of Homeland Security, "Dams Sector Snapshot," 2010, www.dhs.gov/xlibrary/assets/nipp_snapshot_dams.pdf, accessed June 1, 2011.
[160] (U) National Dam Safety Review Board, Independent Panel of Engineers, "Report on Breach of Delhi Dam," December 1, 2010, www.iowadnr.gov/water/floodplain/files/delhi_report.pdf, accessed June 1, 2011. See, among others, the failure of Iowa's Delhi Dam in 2010 following heavy rainfall and overtopping.
[161] (U) National Committee on Levee Safety, "Draft Recommendations for a National Levee Safety Program: A Report to Congress from the National Committee on Levee Safety," January 15, 2009, www.nfrmp.us/ncls/docs/NCLS-Recommendation-Report_012009_DRAFT.pdf, accessed on April, 26, 2011.
[162] (U) Geotechnical Extreme Events Reconnaissance, "Preliminary Observations of the Fujinuma Dam Failure Following the March 11, 2011 Tohoku Offshore Earthquake, Japan," June 6, 2011,

www.geerassociation.org/GEER_Post%20EQ%20Reports/Tohoku_Japan_2011/QR5_Preliminary%20Observations%20of%20Fujinuma%20Dam%20Failure_(06-06-11).pdf, accessed on June 14, 2011.
[163] (U//FOUO) Department of Homeland Security, *2010 Sector CIKR Protection Annual Report for the Dams Sector,* "Sector Risk Considerations," June 2010.
[164] (U//FOUO) Department of Homeland Security, Office of Intelligence and Analysis, "Terrorist Tactic: Water-Borne Improvised Explosive Devices," March 4, 2011.
[165] (U//FOUO) Department of Homeland Security, *2010 Sector CIKR Protection Annual Report for the Dams Sector,* "Sector Risk Considerations," June 2010.
[166] (U) Hydroworld, "Attack on hydropower station in Russia leaves two dead, damages plant," July 21, 2010, www.hydroworld.com/index/display/article-display/9764384543/articles/hrhrw/News-2/2010/07/attack-on_hydropower.html, accessed on June 14, 2011.
[167] (U) Based on searches of the START Global Terrorism database, www.start.umd.edu/gtd/, accessed on April 26, 2011, and the NCTC Worldwide Incident Tracking System, https://wits.nctc.gov/FederalDiscoverWITS/, accessed on April 26, 2011.
[168] (U) American Society of Civil Engineers (ASCE), *2009 Report Card for America's Infrastructure*, Reston, VA: American Society of Civil Engineers, 2009, accessed at www.infrastructurereportcard.org/report-cards, accessed April 26, 2011.
[169] (U) Ibid.
[170] (U) Ibid.
[171] (U) Department of Homeland Security, *Dams Sector-Specific Plan*, 2010.
[172] (U) Department of Homeland Security, "Defense Industrial Base Snapshot," www.dhs.gov/xlibrary/assets/nipp_snapshot_defenseindustrialbase.pdf, accessed May 10, 2011.
[173] (U) Department of Homeland Security and Department of Defense, *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf, accessed June 1, 2011.
[174] (U) Department of Defense, Defense Security Service, "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," 2010, http://dssa.dss.mil/counterintel/2010/DSS_Unclassified.pdf, accessed May 10, 2011.
[175] (U//FOUO) Department of Homeland Security and Department of Defense, *2010 Sector CIKR Protection Annual Report for the Defense Industrial Base,* "Sector Risk Considerations," June 2010.
[176] (U) Ibid.
[177] (U) Ibid.
[178] (U) Mcafee and Center for Strategic & International Studies, "In the Dark: Crucial Industries Confront Cyberattacks," April 2011, www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf, accessed May 10, 2011.
[179] (U) Department of Defense, Defense Security Service, "Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry," 2010, http://dssa.dss.mil/counterintel/2010/DSS_Unclassified.pdf, accessed May 10, 2011.
[180] (U//FOUO) Department of Homeland Security and Department of Defense, *2010 Sector CIKR Protection Annual Report for the Defense Industrial Base,* "Sector Risk Considerations," June 2010.
[181] (U) U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, *Defense Industrial Base Assessment: Counterfeit Electronics,* January 2010, www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf, accessed May 10, 2011.
[182] (U) Grow, B., T. Chi-chu, C. Edwards, and B. Burnsed, Bloomberg Business Week, "Dangerous Fakes," October 2, 2008, www.businessweek.com/magazine/content/08_41/b4103034193886.htm, accessed May 10, 2011.
[183] (U) Department of Homeland Security and Department of Defense, *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf, accessed May 10, 2011.
[184] (U) Department of Homeland Security, "Emergency Services Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189094187811.shtm, accessed June 20, 2011.
[185] (U) Department of Homeland Security Emergency Services Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf, accessed on June 21, 2011.
[186] (U) International Telecommunications Union News, "Satellite communications to bolster emergency response," www.itu.int/net/itunews/issues/2011/02/34.aspx , accessed on June 21, 2011.
[187] (U) Government Accountability Office, "First Responders: Much Work Remains to Improve Communications Interoperability," April 2007, www.gao.gov/new.items/d07301.pdf, accessed on June 21, 2011.
[188] (U) National Academy of Engineering,www.nae.edu/Publications/TheBridge/Archives/19804/20091.aspx,2010
[189] (U) Reuters, "Anthrax scare briefly closes ABC News Office," www.reuters.com/article/2007/06/16/us-anthrax-idUSN1528187420070616, accessed June 21, 2011.
[190] (U) Maniscalco, Paul M. and Christen, Hank T., *Homeland Security: Principles and Practice of Terrorism Response*, Sudbury, MA: Jones & Bartlett Learning, 2010.
[191] (U) Reuters, "Factbox: Congresswoman Gabrielle Giffords shot," www.reuters.com/article/2011/01/08/us-usa-shooting-congresswoman-factbox-idUSTRE70723F20110108, accessed on June 21, 2011.
[192] (U) Rivera, Ray and Sahak, Sharifullah, "Five Arrests in Attack on Hospital in Kabul," *The New York Times*, www.nytimes.com/2011/05/24/world/asia/24afghanistan.html, accessed on June 21, 2011.
[193] (U) U.S. Department of Homeland Security and Department of Energy, *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010.*
[194] (U//FOUO) Department of Homeland Security and Department of Energy, 2010 Energy Sector CIKR Protection Annual Report, draft, May 3, 2010.

[195] (U) Bloomberg, "Energy Infrastructure Lacks Advanced Defense From Cyber Attacks", April 6, 2011, www.bloomberg.com/news/print/2011-04-06/energy-infrastructure-lacks-advanced-defense-from-cyber-attacks.html, accessed June 21, 2011.
[196] (U) NCTC Worldwide Incident Tracking System, https://wits.nctc.gov/FederalDiscoverWITS/index.do?Rd=FacilitiesType%7C4294967143%7CEnergy+Infrastructure&t=Records&Nrc=id+8074+dynrank+disabled&N=0, accessed June 21, 2011.
[197] (U//FOUO) Department of Homeland Security and Department of Energy, 2010 Energy Sector CIKR Protection Annual Report, draft, May 3, 2010.
[198] (U) U.S. Energy Information Administration, "2010 Outlook for Hurricane-Related Production Outages in the Gulf of Mexico," June 2010, www.eia.gov/steo/special/pdf/2010_sp_03.pdf, accessed June 21, 2011.
[199] (U) U.S. Department of Homeland Security and Department of Energy, *Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010*.
[200] (U) U.S Department of Agriculture, Louisiana Field Office, *Louisiana Farm Reporter,* Baton Rouge, LA: USDA, 11(6)(2011) www.nass.usda.gov/Statistics_by_State/Louisiana/Publications/Farm_Reporter/Ff031711.pdf, accessed April 13, 2011.
[201] (U) U.S. Food and Drug Administration, *Food Facilities Registration Statistics,* December 1, 2010, www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/RegistrationofFoodFacilities/ucm236512.htm, accessed April 14, 2011.
[202] (U) U.S. Department of Agriculture, Food and Drug Administration, and DHS Office of Infrastructure Protection, *Sector Specific Plan: Agriculture and Food*, Washington, D.C.: U.S. Department of Homeland Security, May 2007.
[203] (U) Centers for Disease Control, *Estimates of Foodborne Illness in the United States*, Atlanta, Georgia: U.S. Department of Health and Human Services, December 15, 2010, www.cdc.gov/foodborneburden/index.html, accessed May 8, 2011.
[204] (U) Scallan, E., Hoekstra, R.M., Angulo, F.J., Tauxe, R.V., Widdowson, M-A., Roy, S.L., et al., "Foodborne Illness Acquired in the United States: Major Pathogens," U.S. Centers for Disease Control Emerging Infectious Diseases 17(1)(2011): 7-15 www.cdc.gov/EID/content/17/1/7.htm, accessed May 9, 2011.
[205] (U) Scallan, E., Griffin, P.M., Angulo, F.J., Tauxe, R.V., and R.M. Hoekstra, "Foodborne Illness Acquired in the United States: Unspecified Agents," U.S. Centers for Disease Control Emerging Infectious Diseases 17(1)(2011): 16-22, www.cdc.gov/eid/content/17/1/16.htm, accessed May 9, 2011.
[206] (U) Batz, M.B. , Hoffmann, S., and J.G. Morris, Jr., *Ranking the Risks: The 10 Pathogen-Food Combinations With The Greatest Burden on Public Health,* Gainesville, Florida: University of Florida, Emerging Pathogens Institute, April 2011, www.epi.ufl.edu/?q=RankingTheRisks, accessed May 9, 2011.
[207] (U) U.S. Food and Drug Administration, "Introduction to Food Security Awareness," *Training Continuation Courses*, 2007, www.fda.gov/Training/ForStateLocalTribalRegulators/ucm120951.htm, accessed May 9, 2011.
[208] (U) Department of Homeland Security Office of Infrastructure Protection, *National Risk Estimate: Global Supply Chain Risk*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[209] (U) CIA Directorate of Intelligence, *Terrorist CBRN: Materials and Effects,* Washington, D.C: Central Intelligence Agency, May 2003, www.cia.gov/library/reports/general-reports-1/CBRN_threat.pdf, accessed May 9, 2011.
[210] (U) Tucker, J.B., *Historical Trends Related to Bioterrorism: An Empirical Analysis*, U.S. Centers for Disease Control Emerging Infectious Diseases 5(4)(1999): 498-504, www.cdc.gov/ncidod/eid/vol5no4/tucker.htm, accessed May 9, 2011.
[211] (U) USDA Economic Research Service, "Economic Impacts on Foreign Animal Disease," *Economic Research Report* (57), Washington, D.C.: U.S. Department of Agriculture, May 2008.
[212] (U) Tabuchi, H., "Disease Threatens Japan's Beef Trade," *The New York Times*, June 11, 2010, www.nytimes.com/2010/06/12/business/global/12beef.html, accessed May 9, 2011.
[213] (U) Carpenter, T.E., O'Brien, J.M., Hagerman, A.D., and B.A. McCarl, "Epidemic and Economic Impacts of Delayed Detection of Foot-and-Mouth Disease: A Case Study of a Simulated Outbreak in California, " Journal of Veterinary Diagnostic Investigation (23)(2011): 26–33, http://fazd.tamu.edu/2011/01/files/2011/01/Epidemic-and-economic-impacts-of-delayed-detection-of-foot-and-mouth-disease.pdf, accessed May 9, 2011.
[214] (U) U.S. Environmental Protection Agency, "Agriculture and Food Supply," *Climate Change – Health and Environmental Effects*, www.epa.gov/climatechange/effects/agriculture.html, accessed May 9, 2011.
[215] (U) U.S. Department of Agriculture, Climate Change, www.usda.gov/oce/climate_change/index.htm, accessed May 9, 2011.
[216] (U) U.S. Climate Change Science Program, *Synthesis and Assessment Product 4.3: The Effects of Climate Change on Agriculture, Land Resources, Water Resources and Biodiversity in the United States*, Washington, D.C.: U.S. Department of Agriculture, May 2008, www.usda.gov/oce/climate_change/sap_2007_FinalReport.htm, accessed May 9, 2011.
[217] (U) U.S. Department of Agriculture, Food and Drug Administration, and DHS Office of Infrastructure Protection, *Sector Specific Plan: Agriculture and Food*, Washington, D.C.: U.S. Department of Homeland Security, May 2007.
[218] (U) Department of Homeland Security Office of Infrastructure Protection, *National Risk Estimate: Global Supply Chain Risk*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[219] (U) Government Accountability Office, "Homeland Security: Actions Need to Better Protect National Icons and Federal Office Buildings from Terrorism," http://www.gao.gov/new.items/d05790.pdf, accessed May 10, 2011.
[220] (U) Doherty, Ruth, "Critical Research/Innovation Focus Area Document: Vehicle-Borne Improvised Explosive Devices (VBIED) Detection," DHS, Science and Technology Directorate, http://www.dhs.gov/xlibrary/assets/st_detect_and_defeat_vbied.pdf, accessed May 10, 2011.
[221] (U) Las Vegas Sun, "Courthouse gunhman had history of brushes with law," January 5, 2010, www.lasvegassun.com/news/2010/jan/05/news-conference-scheduled-federal-courthouse/, accessed June 20, 2011.
[222] (U) Baker, Stewart, with Natalia Filipiak and Katrina Timlin, "In the Dark: Crucial Industries Confront Cyberattacks," McAfee second annual critical infrastructure report (written with the Center for Strategic and International Studies), 2011.

[223] (U) Keeney, M., Kowalski, E., Capelli, D., Moore, A., Shimeall, T., and Rogers, S., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," United States Secret Service and Carnegie Mellon CERT Software Engineering Institute, May 2005.
[224] (U) U.S. Department of Health and Human Services and DHS Office of Infrastructure Protection, *Sector Specific Plan: Healthcare and Public Health*, Washington, D.C.: U.S. Department of Homeland Security, 2010, draft.
[225] (U) Ibid.
[226] (U) Ibid.
[227] (U) Department of Homeland Security Office of Infrastructure Protection, *National Risk Estimate: Global Supply Chain Risk*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[228] (U) U.S. Department of Health and Human Services and DHS Office of Infrastructure Protection, *Sector Annual Report: Healthcare and Public Health*, Washington, D.C.: U.S. Department of Homeland Security, 2010, draft.
[229] (U) American Society of Radiologic Technologists, *ASRT Supports Senate Bill for U.S. Isotope Production,* February 2011, www.asrt.org/Content/News/PressRoom/PR2011/IsotopesBill110224.aspx, accessed May 8, 2011.
[230] (U) Business Insurance, *Supply Chain Risks Expanding,* February 2011, www.businessinsurance.com/article/20110227/ISSUE0401/302279974, accessed May 8, 2011.
[231] (U) U.S. Food and Drug Administration Website, "Standards Development for Prescription Drug Supply Chain Security," *Counterfeit Drugs*, www.fda.gov/Drugs/DrugSafety/ucm169828.htm, accessed May 9, 2011.
[232] (U) U.S. Department of Health and Human Services and DHS Office of Infrastructure Protection, *Sector Annual Report: Healthcare and Public Health*, Washington, D.C.: U.S. Department of Homeland Security, 2010, draft.
[233] (U) Ibid.
[234] (U) USA Today, *Hopkins Shooting Makes Caregivers Aware of Stresses, Vulnerabilities*, September 2010, www.usatoday.com/news/health/2010-09-20-Hopkinsshooting19_ST_N.htm#, accessed May 9, 2011.
[235] (U) FOXNews, *FBI Probes Hacker's $10 Million Ransom Demand for Stolen Virginia Medical Records,* May 2009, www.foxnews.com/story/0,2933,519187,00.html, accessed May 8, 2011.
[236] (U) Forbes, *How Safe are Your Medical Records?,* June 2009, www.forbes.com/2009/06/03/health-identity-theft-lifestyle-health-medical-records.html, accessed May 8, 2011.
[237] (U) Healthcare IT News, *Balancing Hospital Security 'Tricky'*, 3 February 2010, accessed 9 May 2011 at www.healthcareitnews.com/news/balancing-hospital-security-%E2%80%98tricky%E2%80%99.
[238] (U) U.S. Department of Health and Human Services and DHS Office of Infrastructure Protection, *Sector Specific Plan: Healthcare and Public Health*, Washington, D.C.: U.S. Department of Homeland Security, 2010, draft.
[239] (U) U.S. Department of Health and Human Services, *HHS Pandemic Influenza Plan,* Washington, D.C.: U.S. Department of Health and Human Services, November 2005.
[240] (U) Pandemic and All-Hazards Preparedness Act, Public Law 417, 109th Congress, December 19, 2006, www.gpo.gov/fdsys/pkg/PLAW-109publ417/html/PLAW-109publ417.htm, accessed May 8, 2011.
[241] (U) U.S. Centers for Disease Control and Prevention, *The 2009 H1N1 Pandemic: Summary Highlights, April 2009-April 2010*, Atlanta, G.A.: U.S. Department of Health and Human Services, June 16, 2010, www.cdc.gov/h1n1flu/cdcresponse.htm, accessed June 20, 2011.
[242] (U) U.S. Department of Health and Human Services and DHS Office of Infrastructure Protection, *Sector Annual Report: Healthcare and Public Health*, Washington, D.C.: U.S. Department of Homeland Security, 2010, draft.
[243] (U) Ibid.
[244] (U) Information Technology Sector Coordinating Council and the Information Technology Government Coordinating Council, *Information Technology Sector Risk Baseline Assessment*, US Department of Homeland Security, Washington, DC, 2009, accessed at http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf on April 22, 2011.
[245] (U) Information Technology Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, US Department of Homeland Security, Washington, DC, 2010, accessed at www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech-2010.pdf on June 10, 2011.
[246] (U) Symantec, "Symantec Internet Security Threat Report," April 2011, www.symantec.com/business/threatreport/index.jsp, accessed May 10, 2011.
[247] (U) Information Technology Sector Coordinating Council and the Information Technology Government Coordinating Council, *Information Technology Sector Risk Baseline Assessment*, US Department of Homeland Security, Washington, DC, 2009, accessed at www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf on April 22, 2011.
[248] (U) Government Accountability Office, "Homeland Security: Actions Need to Better Protect National Icons and Federal Office Buildings from Terrorism," http://www.gao.gov/new.items/d05790.pdf, accessed May 10, 2011.
[249] (U) Doherty, Ruth, "Critical Research/Innovation Focus Area Document: Vehicle-Borne Improvised Explosive Devices (VBIED) Detection," DHS, Science and Technology Directorate, http://www.dhs.gov/xlibrary/assets/st_detect_and_defeat_vbied.pdf, accessed May 10, 2011.
[250] (U) Ibid, pp. 4-5.
[251] (U) Department of Homeland Security National Monuments and Icons Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf, accessed June 21, 2011.
[252] (U) Government Accountability Office, *Homeland Security: Actions Needed to Improve Security Practices at National Icons and Parks*, www.gao.gov/new.items/d09983.pdf, accessed on Jun 24, 2011.
[253] Ibid.
[254] Ibid.
[255] (U) Department of Homeland Security, National Monuments and Icons Sector-Specific Plan, www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf, accessed June 21, 2011.
[256] (U) Department of Homeland Security, "Nuclear Reactors, Materials, and Waste Sector Snapshot," www.dhs.gov/xlibrary/assets/nipp_snapshot_nuclear.pdf, accessed May 2, 2011.

[257] (U//FOUO) Department of Homeland Security and Department of Defense, *2010 Sector CIKR Protection Annual Report for the Nuclear Sector,* "Sector Risk Considerations," June 2010.
[258] (U) Alvarez, Robert, *Spent Nuclear Fuel Pools in the U.S.: Reducing the Deadly Risks of Storage*, Institute for Policy Studies, May 2011.
[259] (U) Nuclear Energy Institute, "Nuclear Power Plant Security, August 2010, www.nei.org/resourcesandstats/documentlibrary/safetyandsecurity/factsheet/powerplantsecurity/?print=true, accessed May 9, 2011.
[260] (U) Department of Homeland Security, National Cyber Security Division, "Threat: Stuxnet," Undated PowerPoint.
[261] (U) National Research Council, *Radiation Source Use and Replacement,* Washington, Committee on Radiation Source Use and Replacement, National Academies Press, Washington, DC, 2008, www.nap.edu/catalog.php?record_id=11976, accessed May 2, 2011.
[262] (U) Senate Committee on Energy and Natural Resources, "**T**estimony on the American Medical Isotopes Production Act of 2011," February 1, 2011, http://nnsa.energy.gov/mediaroom/congressionaltestimony/staplestestimony2111, accessed April 27, 2011.
[263] (U) Department of Homeland Security, "Nuclear Sector Overview," www.dhs.gov/files/programs/gc_1188475350325.shtm, accessed May 2, 2011.
[264] (U) U.S. Department of Homeland Security, *Postal and Shipping Sector Snapshot*, Washington, D.C.: Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_snapshot_postal.pdf, accessed April 29, 2011.
[265] (U) Ibid, accessed May 27, 2011.
[266] (U) Ibid, accessed May 27, 2011.
[267] (U) Ibid, accessed April 29, 2011.
[268] (U) Ibid, accessed June 21, 2011.
[269] (U) Hope, Karin and Stanley Pinal, "Greece halts mail services after attacks," Financial Times, November 3, 2010, www.ft.com/cms/s/0/c41969ac-e752-11df-880d-00144feab49a.html#axzz1NYqxy0mq, accessed May 27, 2011.
[270] (U) CBS News, "Italian anarchists claim Greek, Swiss mail bombs," April 1, 2011, www.cbsnews.com/stories/2011/04/01/ap/europe/main20049621.shtml, accessed May 27, 2011.
[271] (U) CNN, "Yemen-based al Qaeda group claims responsibility for parcel bomb plot," November 6, 2010, http://edition.cnn.com/2010/WORLD/meast/11/05/yemen.security.concern/?hpt=T2, accessed June 21, 2011.
[272] (U) BBC, "Air freight from Yemen and Somalia banned, November 1, 2010, http://www.bbc.co.uk/news/uk-11669636, accessed June 21, 2011.
[273] (U//FOUO) Department of Homeland Security, *Postal and Shipping: Critical Infrastructure and Key Resources Sector Specific Plan,* 2007.
[274] (U) United States Postal Service, *USPS Tallies Terror Costs for Congress*, Washington, D.C.: United States Postal Service, www.usps.com/news/2001/press/pr01_1108aid.htm, accessed April 29, 2011.
[275] (U) U.S. Department of Homeland Security, *Postal and Shipping Sector Snapshot*, Washington, D.C.: Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_snapshot_postal.pdf, accessed April 29, 2011.
[276] (U) U.S. Department of Homeland Security, *Transportation Systems Sector-Specific Plan,* Washington, D.C.: Department of Homeland Security, May 2007.
[277] (U) Testimony of Secretary Janet Napolitano, House Committee on Homeland Security, Understanding the Homeland Threat Landscape – Considerations for the 112th Congress, 112th Congress, 1st sess., 2011, www.dhs.gov/ynews/testimony/testimony_1297263844607.shtm.
[278] (U) Levin, Peter, "Fear and heroism aboard Northwest Airlines Flight 253 after attempted bombing," Washington Post, December 27, 2009, www.washingtonpost.com/wp-dyn/content/article/2009/12/26/AR2009122601150.html, accessed May 27, 2011.
[279] (U) Testimony of TSA Administrator John S. Pistol, House Committee on Homeland Security, Terrorism and Transportation Security (TSA Oversight), 112th Congress, 1st sess., 2011, homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Pistole.pdf.
[280] (U) BBC, "Belarus: Blast rocks Minsk metro near Lukashenka office," April 11, 2011, http://www.bbc.co.uk/news/world-europe-13042316, accessed May 31, 2011.
[281] (U) BBC, "Moscow Metro hit by deadly suicide bombings," March 29, 2010, http://news.bbc.co.uk/2/hi/8592190.stm, accessed May 31, 2011.
[282] (U) BBC, "Mumbai bombings suspects charged," November 30, 2006, http://news.bbc.co.uk/2/hi/south_asia/6159373.stm, accessed June 14, 2011.
[283] (U) Frankel, Glenn, "Bombers Strike London at Rush Hour," Washington Post, July 8, 2005, www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070702390.html, accessed May 31, 2011.
[284] (U) BBC, "Moscow on edge after bomb horror," February 6, 2004, http://news.bbc.co.uk/2/hi/europe/3467645.stm, accessed June 14, 2011.
[285] (U) Richburg, Keith B., "Madrid Train Blasts Kill at Least 190," Washington Post, March 12, 2005, www.washingtonpost.com/wp-dyn/content/article/2007/08/09/AR2007080901428.html, accessed May 31, 2011.
[286] (U) Department of Homeland Security and U.S. Environmental Protection Agency, *Sector Annual Report: Water*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[287] (U) Ibid.
[288] (U) Safe Drinking Water Act, Pub's. 93-523; 88 Stat. 1660; 42 U.S.C. § 300f *et seq*. 1974-12-16.
[289] (U) U.S. Environmental Protection Agency, "National Primary Drinking Water Regulations," *Code of Federal Regulations,* 40 CFR Part 141.
[290] (U) George W. Bush, *The President's State of the Union Address*, The United States Capitol, Washington, D.C., January 29, 2002, georgewbush-whitehouse.archives.gov/news/releases/2002/01/20020129-11.html, accessed May 13, 2011.
[291] (U) Federal Bureau of Investigation, Terrorism: Are Our Water Resources and Environment at Risk? Hearing before the Subcommittee on Water Resources and Environment of the Committee on Transportation and Infrastructure, House of

Representatives, 107th Congress, 1st session (107-51) October 10, 2001, www.fbi.gov/news/testimony/terrorism-are-americas-water-resources-and-environment-at-risk, accessed May 13, 2011.
[292] (U) U.S. Centers for Disease Control and Prevention, *Water-related Diseases, Contaminants, and Injuries*, updated January 25, 2010, www.cdc.gov/healthywater/disease/, accessed May 13, 2011.
[293] (U) Coors, P.S., Kramer, M.H., Blair, K.A., Addis, D.G., Davis, J.P., and A.C. Addax, "Cost of illness in the 1993 Waterborne *Cryptosporidium* outbreak, Milwaukee, Wisconsin," *Emerge Infect Dies 9(4),* Atlanta, GA: U.S. Department of Health and Human Services, *2003,* www.cdc.gov/ncidod/EID/vol9no4/02-0417.htm, accessed June 20, 2011
[294] (U) Department of Homeland Security and Environmental Protection Agency, *Sector Annual Report: Water*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[295] (U) Ibid.
[296] (U) Mississippi Rural Water Association, *Mara Responds After Tornados,* Duncan, O.K.: National Rural Water Association, May 13, 2011, www.nrwa.org/NRWAUpdates/2011%2005%20May/Misstornado.htm, accessed June 20, 2011.
[297] (U) Department of Homeland Security and Environmental Protection Agency, *Sector Specific Plan: Water*, Washington, D.C.: U.S. Department of Homeland Security, 20010, draft.
[298] (U) Water Infrastructure Security Enhancements (WISE) Initiative, *Recovery Practices Primer for Natural Disasters,* September 2008, *www.awwa.org/files/science/WISE/6.pdf, accessed May 13, 2011.*
[299] (U) Natural Resources Defense Council, "Report: More than One Out of Three U.S. Counties Face Water Shortages Due to Climate Change," *Press Release,* July 20, 2010, www.nrdc.org/media/2010/100720.asp, accessed May 13, 2011.
[300] (U) Environmental Protection Agency, *Water Supply and Use in the United States,* Washington, D.C.: U.S. Environmental Protection Agency, June 2008, www.epa.gov/WaterSense/pubs/supply.html, accessed May 13, 2011.
[301] (U) Department of Homeland Security and Environmental Protection Agency, *Sector Annual Report: Water*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[302] (U) Ibid.
[303] (U) Federal Bureau of Investigation, *Threats and Consequences of Cyber Attacks on U.S. Water Sector Industrial Control Systems*, Washington, D.C.: U.S. Department of Justice, September 14, 2010.
[304] (U) Department of Homeland Security and Environmental Protection Agency, *Sector Specific Plan: Water*, Washington, D.C.: U.S. Department of Homeland Security, 20010, draft.
[305] (U) Abrams, M., and J. Weiss, *Malicious Control System Cyber Security Attack Case Study–Mariachi Water Services, Australia*, 2008, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf, accessed June 20, 2011.
[306] (U) Department of Homeland Security and Environmental Protection Agency, *Sector Annual Report: Water*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[307] (U) School, Renee, "Utilities, investors face risks from growing water scarcity," *McClatchy Newspapers*, 21 October 2010, accessed at http://www.mcclatchydc.com/2010/10/21/102355/utilities-investors-face-risks.html#ixzz13077nHwV on February 11, 2011.
[308] (U) Department of Homeland Security and Environmental Protection Agency, *Sector Annual Report: Water*, Washington, D.C.: U.S. Department of Homeland Security, 2011, draft.
[309] (U) Federal Emergency Management Agency, www.fema.gov/news/disasters.fema, accessed 18 May 2011.
[310] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[311] (U) Ibid.
[312] (U) Federal Emergency Management Agency, *Region I,*www.fema.gov/about/regions/regioni, accessed 18 May 2011.
[313] (U) The Northeast States Emergency Consortium (NESEC), Winter Storms website, www.nesec.org/hazards/winter_storms.cfm, accessed 24 May 2011.
[314] (U) Strauss, Neil. "The Great Northeast Blizzard of 1978 Remembered 30 Years Later in Southern New England." National Oceanic and Atmospheric Administration, www.erh.noaa.gov/box/papers/blizzard78/mainblizzardof78.htm, accessed 24 May 2010.
[315] (U) Federal Emergency Management Agency, *Region I,*www.fema.gov/about/regions/regioni, accessed 18 May 2011.
[316] (U) Ibid.
[317] (U) The Northeast States Emergency Consortium (NESEC), Winter Storms website, www.nesec.org/hazards/winter_storms.cfm, accessed 24 May 2011.
[318] (U) Ibid.
[319] (U) The Northeast States Emergency Consortium, *Hurricanes*, www.nesec.org/hazards/hurricanes.cfm, accessed 27 June 2011.
[320] (U) The New England Council, www.newenglandcouncil.com/issues/transportation, accessed 25 May 2011.
[321] (U) Bureau of Economic Analysis Gross Domestic Product (GDP) by Metropolitan Area for Industries, 2009.
[322] (U) U.S. Department of Transportation, Press Release, U.S. Transportation Secretary LaHood Announces $2 Billion for High-Speed Intercity Rail Projects to Grow Jobs, Boost U.S. Manufacturing and Transform Travel in America," 9 May 2011, www.dot.gov/affairs/2011/dot5711.html, accessed 25 May 2011.
[323] (U) Ibid.
[324] (U) Statement of John S. Pistol, Administrator, Transportation Security Administration, before the Senate Committee on Commerce, Science and Transportation, "Emerging Threats to Rail Security," 14 June 2011.
[325] (U//FOUO) Department of Homeland Security and Federal Bureau of Investigation, Joint Intelligence Bulletin, "Early 2010 Al-Qa'ida Interest in Targeting Trains on 11 September 2011," 5 May 2011.
[326] (U) Anderson, Patrick and Ileana Gecko. AEG Working Paper: Economic Impact of 2003 Blackout, Anderson Economic Group, 19 August 2003.
[327] (U) ISO-New England, "ISO New England Forecasts Adequate Resources to Meet Summer Electricity Demand," 28 April 2011, www.iso-ne.com/nwsiss/pr/2011/2011_summer_outlook.pdf, accessed 25 May 2011.

[328] (U) Federal Energy Regulatory Commission, Electric Power Markets: New England (ISO-NE), www.ferc.gov/market-oversight/mkt-electric/new-england.asp, accessed 25 May 2011.
[329] (U) Reuters, "Green Mountain to buy power from N.H. Seabrook nuke," 25 May 2011, www.reuters.com/article/2011/05/25/utilities-greenmountain-nextera-seabrook-idUSN2510350620110525, accessed 25 May 2011.
[330] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed on 17 May 2011.
[331] (U) Ibid.
[332] (U/FOUO) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[333] (U) Federal Emergency Management Agency, www.fema.gov/news/disasters.fema, accessed 18 May 2011.
[334] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[335] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[336] (U) Ibid.
[337] (U) New York City Natural Hazard Mitigation Plan, March 2009
[338] (U) Ibid.
[339] (U) City of New York, Office of the Comptroller/Office of Policy Management, "The Endless Winter: Fiscal and Economic Effects of NYC's Record 52-Foot Snows of 1995-96," www.comptroller.nyc.gov/bureaus%2Fopm/h9b.shtm, accessed 25 May 2011.
[340] (U//FOUO) Department of Homeland Security, Office of Intelligence & Analysis, New York: State Critical Infrastructure Threat Assessment. October 2008.
[341] (U) Ibid.
[342] (U) Ibid.
[343] (U) Ibid.
[344] (U) McCarter, Mickey. "TSA Calls for Increased Vigilance Due to Threat of Rail Plot," Homeland Security Today, 9 May 2011, http://www.hstoday.us/briefings/today-s-news-analysis/single-article/tsa-calls-for-increased-vigilance-due-to-threat-of-rail-plot/ee3a737e6470b70bf35d05bc696c3c82.html, accessed 25 May 2011
[345](U//FOUO) Department of Homeland Security, Office of Intelligence & Analysis, New York: State Critical Infrastructure Threat Assessment. October 2008.
[346] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/,,accessed on 17 May 2011.
[347] (U) Ibid.
[348] (U//FOUO) Department of Homeland Security, Office of Infrastructure Protection, "Infrastructure Protection Note: Evolving Threats to the Homeland," 24 May 2010.
[349] (U//FOUO) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[350] (U) Federal Emergency Management Agency , "Region III," www.fema.gov/about/regions/regioniii/, accessed 25 May 2011.
[351] (U) Federal Emergency Management Agency, "Federal Disaster Declarations," www.fema.gov/news/disasters.fema, accessed 19 May 2011.
[352] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[353] (U) Ibid.
[354] (U) Federal Emergency Management Agency, "Federal Disaster Declarations," www.fema.gov/news/disasters.fema, accessed 23 May 2011.
[355] (U) Bloomberg Business Week, "Power outages hit DC area after storms; 2 dead,"26 July 2010, www.businessweek.com/ap/financialnews/D9H6PMM80.htm, accessed 25 May 2010.
[356] (U) Washington Post, "Historic snowstorm in D.C. leaves a mess to be reckoned with," 7 February 2010, www.washingtonpost.com/wp-dyn/content/article/2010/02/06/AR2010020600683.html?sid=ST2010021903762, accessed 25 May 2011.
[357] (U) Richmond Times-Dispatch, "Snowfall ends; citizens urged to stay home," 6 February 2010, www2.timesdispatch.com/news/2010/feb/06/snowfall_ends_citizens_urged_to_stay_home-ar-11375/, accessed 25 May 2011.
[358] (U) Washington Post, "Snow-related shutdowns cost less than expected, OPM chief says," 24 March 2010, www.washingtonpost.com/wp-dyn/content/article/2010/03/23/AR2010032304036.html, accessed 25 May 2011.
[359] (U) Washington Metropolitan Area Transit Authority, "215 million people rode Metrorail in fiscal year 2008," www.wmata.com/about_metro/news/PressReleaseDetail.cfm?ReleaseID=2179, accessed 25 May 2011.
[360] (U) Washington Post, "Feds arrest N.VA. man in D.C. Metro bomb plot," 28 October 2010, www.washingtonpost.com/wp-dyn/content/article/2010/10/27/AR2010102704857.html, accessed 25 May 2011.
[361] (U) Federal Bureau of Investigation, "Arlington Man Indicted for Alleged Threats via Facebook," 5 January 2011, www.fbi.gov/washingtondc/press-releases/2011/wfo010511.htm, accessed 25 May 2011.
[362] (U) White House, "High-Speed Intercity Passenger Rail Program, Northeast Region," undated, www.whitehouse.gov/sites/default/files/rail_northeast.pdf, accessed 25 May 2011.
[363] (U//FOUO) Department of Homeland Security and Federal Bureau of Investigation, Joint Intelligence Bulletin, "Early 2010 Al-Qa'ida Interest in Targeting Trains on 11 September 2011," 5 May 2011.

[364] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed 25 May 2011.
[365] (U) Ibid.
[366] (U//FOUO) Department of Homeland Security and Federal Bureau of Investigation, Joint Intelligence Bulletin, "February 2010 Al-Qa'ida Homeland Plotting Priorities Included Symbolic Dates and Major U.S. Cities," 20 May 2011.
[367] (U) Federal Bureau of Investigation, "Maryland Man Charged in Plot to Attack Armed Forces Recruiting Center," 8 December 2010, www.fbi.gov/baltimore/press-releases/2010/ba120810.htm, accessed 25 May 2011.
[368] (U) Environmental Protection Agency, *The Delaware Estuary,* http://water.epa.gov/lawsregs/lawsguidance/cwa/316b/phase2/upload/chb1.pdf , accessed 27 June 2011.
[369] (U//FOUO) Department of Homeland Security, National Critical Infrastructure Prioritization Program.
[370] (U) Federal Emergency Management Agency, "Region IV," www.fema.gov/about/regions/regioniv/index.shtm, accessed 19 May 2011.
[371] (U) Federal Emergency Management Agency, "Federal Disaster Declarations," www.fema.gov/news/disasters.fema, accessed 19 May 2011.
[372] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[373] (U) Ibid.
[374] (U) Federal Emergency Management Agency, "Region IV," www.fema.gov/about/regions/regioniv/index.shtm, accessed 23 May 2011.
[375] (U) Federal Emergency Management Agency, "Federal Disaster Declarations," www.fema.gov/news/disasters.fema, accessed 23 May 2011.
[376] (U) Ibid.
[377] (U) National Committee on Levee Safety, "Draft Recommendations for a National Levee Safety Program: A Report to Congress from the National Committee on Levee Safety," January 15, 2009, www.nfrmp.us/ncls/docs/NCLS-Recommendation-Report_012009_DRAFT.pdf, accessed April, 26, 2011.
[378] (U) Department of Homeland Security, *Commercial Facilities Sector: Critical Infrastructure and Key Resources*, www.dhs.gov/files/programs/gc_1189101907729.shtm, accessed 13 May 2011.
[379] (U) Committee on Homeland Security, Public Health, Safety, and Security for Mass Gatherings, US House of Representatives, May 2008, accessed at http://chsdemocrats.house.gov/SiteDocuments/20080513105623-98169.pdf on June 14, 2011.
[380] (U) National Retail Federation, "NRF-ICSC Emergency Response Protocols to Active Shooters," 2008, www.lpinformation.com/Portals/0/NRF_ActiveShooter_Guidelines.pdf, accessed 13 May 2011.
[381] (U//FOUO) National Infrastructure Simulation and Analysis Center, "Hurricane Gustav Supplemental Analysis Summary, 13 September 2008, 0300 EDT.
[382] (U//FOUO) National Infrastructure Simulation and Analysis Center, "Hurricane Gustav Chemical and Transportation Analysis Update, 2 September 2009, 0300 EDT.
[383] (U) Plastics Today, "Katrina Spins U.S. Petrochemicals Into Disarray," 7 September 2005, www.plasticstoday.com/articles/katrina-spins-us-petrochemicals-disarray, accessed 24 May 2011.
[384] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed 23 May 2011.
[385] (U//FOUO) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[386] (U) Federal Emergency Management Agency, *Annual Major Disaster Declarations Totals*, www.fema.gov/news/disaster_totals_annual.fema, accessed on May 25, 2011.
[387] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation," "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," www.data.gov, accessed on May 27, 2011.
[388] (U) Federal Emergency Management Agency, *FEMA News*, www.fema.gov/femaNews/disasterSearch.do?action=Bookmark&searchPublished=1&sortBy=dateDeclared&sortDescending=Y&searchRegionId=5&searchSpanish=0, accessed on 24 May 2011.
[389] (U) Federal Emergency Management Agency, *Annual Major Disaster Declarations Totals*.
[390] (U) National Oceanic and Atmospheric Administration, "Spring Flooding Underway, Expected to Worsen through April," 17 March 2011.
[391] (U) Weather.com, "The Mississippi River Flood of 1993, Storm Encyclopedia," www.weather.com/encyclopedia/flood/miss93.html, accessed 14 June 2011.
[392] (U) Ibid.
[393] (U) U.S. Department of Agriculture, *National Agricultural Statistics Service Data and Statistics*, www.nass.usda.gov/Data_and_Statistics/Pre-Defined_Queries/index.asp, accessed 25 May 2011.
[394] (U) Ibid.
[395] (U) U.S. Department of Agriculture Agricultural Marketing Service, *Grain Transportation Report*, www.ams.usda.gov/AMSv1.0/ams.fetchTemplateData.do?template=TemplateA&navID=AgriculturalTransportation&leftNav=AgriculturalTransportation&page=ATGrainTransportationReport&description=Grain%20Transportation%20Report%20(GTR), accessed on 25 May 2011.
[396] (U//FOUO) Department of Homeland Security: Office of Intelligence and Analysis "Illinois State Threat Assessment," 13 November 2008.
[397] (U) Ibid.
[398] (U) Ibid.

[399] (U) Ibid.
[400] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed 17 May 2011.
[401] (U) American Public Transportation Association, *Ridership Report*, www.apta.com/resources/statistics/Pages/ridershipreport.aspx, accessed on May 25, 2011.
[402] (U) Airports Council International, www.airports.org/cda/aci_common/display/main/aci_content07_c.jsp?zn=aci&cp=1-5-54-55_666_2__, accessed on May 25, 2011.
[403] (U) Government Accountability Office, "Aviation Security: DHS Has Taken Steps to Enhance International Aviation Security and Facilitate Compliance with International Standards, but Challenges Remain," www.gao.gov/new.items/d11238t.pdf, accessed on May 25, 2011.
[404] (U) Reuters, "Al Qaeda plotted 9/11 anniversary rail attack –US," www.reuters.com/article/2011/05/06/uk-usa-security-trains-idUSLNE74500Q20110506, accessed on May 25, 2011.
[405] (U) Federal Emergency Management Agency, www.fema.gov/news/disasters.fema, accessed 18 May 2011.
[406] (U) Blake, Eric S., Edward N. Rappaport, Christopher W. Landsea, "The Deadliest Costliest, and most intense United States Tropical Cyclones from 1851 to 2006 (and other frequently requested hurricane facts)," 15 April 2007, *National Hurricane Center*, National Oceanic and Atmospheric Administration, www.nhc.noaa.gov/pdf/NWS-TPC-5.pdf, accessed 5 May 2011.
[407] (U) U.S. Energy Information Administration, Ranking of U.S. Refineries, September 2010.
[408] (U) U.S. Department of Commerce "Hurricane Katrina Service Assessment Report" June 2006, www.weather.gov/om/assessments/pdfs/Katrina.pdf, accessed 14 May 2011.
[409] (U) Committee on Homeland Security, *Public Health, Safety, and Security for Mass Gatherings,* US House of Representatives, May 2008, accessed at http://chsdemocrats.house.gov/SiteDocuments/20080513105623-98169.pdf on June 14, 2011.
[410] (U) Department of Homeland Security, *Commercial Facilities Sector: Critical Infrastructure and Key Resources*, www.dhs.gov/files/programs/gc_1189101907729.shtm, accessed 13 May 2011.
[411] (U) http://www.fbi.gov/news/stories/2010/november/terror-plot-foiled
[412] (U) USA Today, "Gulf oil spill now largest offshore spill in history as BP continues plug effort," 27 May 2011. www.usatoday.com/news/nation/2010-05-27-oil-spill-news_N.htm?csp=34news, accessed 9 June 2010.
[413] (U) Wearden, Graeme, "BP oil spill costs to hit $40bn," The Guardian, 2 November 2010, www.guardian.co.uk/business/2010/nov/02/bp-oil-spill-costs-40-billion-dollars, accessed 8 June 2011.
[414] (U) Houston Business Journal, "Deepwater Horizon cost Houston massive jobs, investment," 15 April 2011, www.bizjournals.com/houston/print-edition/2011/04/15/deepwater-horizon-cost-houston-massive.html, accessed 28 May 2011.
[415] (U) Deepwater Horizon Study Group, The Macondo Blowout: 3rd Progress Report, Center for Catastrophic Risk Management: University of California Berkeley, December 2010.
[416] (U) Associated Press, "US rig count rises by 1 to 1,855; New Mexico leads with 7 new sites," 10 June 2011, www.washingtonpost.com/business/industries/us-rig-count-rises-by-1-to-1855-new-mexico-leads-with-7-new-sites/2011/06/10/AGk1mBPH_story.html, accessed 14 June 2011.
[417] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed on 17 May 2011.
[418] (U) Ibid.
[419] (U//FOUO) Department of Homeland Security: Office of Intelligence and Analysis "Oklahoma State Threat Assessment," 18 March 2009.
[420] (U) Horswell, Cindy, "FBI issues alert on terror threat to oil refineries," Houston Chronicle, 26 March 2004, www.chron.com/disp/story.mpl/metropolitan/2468502.html, accessed 8 June 2011.
[421] (U//FOUO) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[422] (U) Federal Emergency Management Agency, www.fema.gov/news/disasters.fema, accessed 18 May 2011.
[423] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov..
[424] (U) Ibid.
[425] (U) Federal Emergency Management Agency, *Region VII,*www.fema.gov/about/regions/regionvii, accessed 18 May 2011.
[426] (U) NOAA, Storm Prediction Center, *Tornado Numbers, Deaths, Injuries, and Adjusted Damage,* 1950-1994, www.spc.noaa.gov/archive/tornadoes/st-trank.html, accessed 24 May 2011.
[427] (U) EQECAT, Inc, "Devastating 2011 Tornado Season Continues; Joplin Tornado Could Cost $1-$3 Billion," 24 May 2011, www.eqecat.com/catWatchREV/secureSite/report.cfm?id=321, accessed 24 May 2011.
[428] (U) NOAA, 2011 tornado information, 23 May 2011, http://www.noaanews.noaa.gov/2011_tornado_information.html, accessed 24 May 2011.
[429] (U) Lehmann, Evan and Lauren Morello. "Deadly Joplin, MO., Twister Raises 'Tough,' Costly Questions, Weather Experts Say," *New York Times*, 24 May 2011, www.nytimes.com/cwire/2011/05/24/24climatewire-deadly-joplin-mo-twister-raises-tough-costly-95767.html, accessed 24 May 2011.
[430] (U) U.S. Department of Agriculture, 2009 Sector Financial Indicators Cash Receipts Ranking Data, (2009), www.ers.usda.gov/Data/FarmIncome/firkdmuXLS.htm, accessed 24 May 2011.
[431] (U) U.S. Department of Agriculture, "Total agricultural exports by State, last 5 fiscal years," (2009), www.ers.usda.gov/data/Stateexports, accessed 24 May 2011.
[432] (U//FOUO) Department of Homeland Security, Office of Intelligence and Analysis, Iowa State Critical Infrastructure Threat Assessment, February 2009.
[433] (U) Dykman, Lawrence, United States Government Accountability Office: Testimony Before the Committee on Governmental Affairs, U.S. Senate, "A Threat to Agriculture and the Food Supply," 19 November 2003

[434] (U) Ibid.
[435] (U) Ibid.
[436] (U) Ibid.
[437] (U//FOUO) Department of Homeland Security, Office of Intelligence and Analysis, Kansas State Critical Infrastructure Threat Assessment, December 2008.
[438] (U//FOUO) Department of Homeland Security, Office of Intelligence and Analysis, Iowa State Critical Infrastructure Threat Assessment, March 2009.
[439] (U) Swenson, David. "The Economic Impact of Ethanol Production in Iowa," Iowa State University (January 2008).
[440] (U) Department of Homeland Security, Chemical Sector Snapshot, Washington, D.C.: Department of Homeland Security, May 2007
[441] (U) Ibid.
[442] (U) Ibid.
[443] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed on 17 May 2011.
[444] (U) Ibid.
[445] (U) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[446] (U) Federal Emergency Management Agency, www.fema.gov/news/disasters.fema, accessed 18 May 2011.
[447] (U) Ibid.
[448] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[449] (U) Ibid.
[450] (U) Federal Emergency Management Agency, *Region VIII,*www.fema.gov/about/regions/regionviii, accessed 18 May 2011.
[451] (U) Zuckerman, Laura. "One dead, two missing in Montana floods," Reuters, 24 May 2011 www.reuters.com/article/2011/05/24/us-floods-montana-idUSTRE74N0LB20110524, accessed 14 June 2011.
[452] (U) U.S. Army Corps of Engineers, Flood Risk Management: Fargo-Moorhead Metro, North Dakota and Minnesota, www.mvp.usace.army.mil/fl_damage_reduct/default.asp?pageid=1455, accessed 23 May 2011.
[453] (U) National Oceanic and Atmospheric Administration, "Spring Flooding Underway, Expected to Worsen through April," 17 March 2011, www.noaanews.noaa.gov/stories2011/20110317_springoutlook.html, accessed 22 March 2011.
[454] (U) Ibid.
[455] (U) National Oceanic and Atmospheric Administration, Climate Prediction Center, www.cpc.ncep.noaa.gov/products/assessments/assess_97/rriver.html, accessed 30 May 2011.
[456] (U) Davey, Monica and Kirk Johnson. "Permanent Flood Solutions Just Out of Reach for Fargo," *New York Times*, 29 March 2009, www.nytimes.com/2009/03/30/us/30grand.html, accessed 23 May 2011.
[457] (U) Finley, Bruce. Colorado has more ailing dams, less money to fix them," *Denver Post*, 7 February 2011, www.denverpost.com/news/ci_17314534, accessed 23 May 2011.
[458] (U) U.S. Department of the Interior, Bureau of Reclamation, Horsetooth Reservoir Safety of Dams Activities Final Environmental Assessment, www.usbr.gov/gp/ecao/horsetooth_carter/horsetooth_safety_dams/htchapter2.htm, accessed 23 May 2011.
[459] (U) Goldman, Adam. "Saudi man charged with plotting terror attack researched Colorado dams," Denver Post, 24 February 2011, www.denverpost.com/breakingnews/ci_17472805, accessed 24 May 2011.
[460] (U) Northern Colorado Water Conservancy District, Colorado-Big Thompson Project, www.ncwcd.org/project_features/cbt_main.asp, accessed 24 May 2011.
[461] (U) Central Valley Water Reclamation Facility, A Brief History, www.cvwrf.org/brochure/page3.php, accessed 24 May 2011.
[462] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed on 17 May 2011.
[463] (U) Ibid.
[464] (U) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[465] (U) Region IX serves a population in excess of 36 million people and covers 386,000 square miles with a breadth of more than 8,000 miles. Federal Emergency Management Agency website, www.fema.gov/about/regions/regionix, accessed 17 May 2011.
[466] (U) Federal Emergency Management Agency website, www.fema.gov/news/disasters.fema, accessed 17 May 2011.
[467] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[468] (U) Ibid.
[469] (U) U.S. Geological Survey, "The Uniform California Earthquake Rupture Forecast, Version 2", 2007.
[470] (U) U.S. Geological Survey, "New Study Shows Odds High for Big California Quakes," 14 April 2008, www.usgs.gov/newsroom/article.asp?ID=1914, accessed 12 May 2011.
[471] (U) In 2010, California received a Federal disaster declaration that damaged water control facilities. (FEMA-1911-DR)
[472] (U) U.S. Geological Survey, "Map: Seismicity of California 1990-2006," www.earthquake.usgs.gov/earthquakes/states/california/seismicity.php, accessed 11 May 2011.
[473] (U) Berkeley Seismological Laboratory, Frequently Asked Questions, www.seismo.berkeley.edu/seismo/faq/1989_0.html, accessed 9 May 2011.
[474] (U) Gordon, Peter and James E. Moore, "Economic Impact Analysis of Terrorism Events: Recent Methodological Advances and Findings. Prepared for the OECD/ITF Round Table of 11-12 December 2008 on Security, Risk Perception and Cost-Benefit Analysis. www.internationaltransportforum.org/jtrc/discussionpapers/DP200822.pdf, accessed 17 May 2011.
[475] (U) Department of Homeland Security, National Infrastructure Protection Plan: Commercial Facilities Sector Specific Plan, 2010.

[476] (U//FOUO) Department of Homeland Security: Office of Intelligence and Analysis "California State Threat Assessment," 2 October 2008.
[477] (U) Ibid.
[478] (U) Department of Homeland Security, *Commercial Facilities Sector: Critical Infrastructure and Key Resources*, www.dhs.gov/files/programs/gc_1189101907729.shtm, accessed 13 May 2011.
[479] (U) Committee on Homeland Security, *Public Health, Safety, and Security for Mass Gatherings,* US House of Representatives, May 2008, accessed at http://chsdemocrats.house.gov/SiteDocuments/20080513105623-98169.pdf on June 14, 2011.
[480] (U) Department of Defense: Armed Forces Press Service, "Los Angeles Skyscraper Was Terrorist Target, Bush Says," 9 February, www.defense.gov/news/newsarticle.aspx?id=14900, accessed 17 May 2011.
[481] (U) Department of Homeland Security, Commercial Facilities Sector Specific Plan, 2010, Washington, D.C.: Department of Homeland Security, 2010.
[482] (U) Department of Homeland Security, Transportation Systems Sector-Specific Plan, Washington, D.C.: Department of Homeland Security, 2007.
[483] (U) Pacific Disaster Center
[484] (U) EQE International, "*Hurricanes Andrew and Iniki 1992,"* www.absconsulting.com/resources/Catastrophe_Reports/Hurricane%20Andrew-Iniki-1992.pdf, accessed 17 May 2011.
[485] (U//FOUO) Department of Homeland Security: Office of Intelligence and Analysis "California State Threat Assessment," 2 October 2008.
[486] (U) House Committee on Homeland Security, Testimony of Secretary Janet Napolitano: Understanding the Homeland Threat Landscape – Considerations for the 112th Congress, 112th Congress, 1st sess., 2011, 9 February 2011, www.dhs.gov/ynews/testimony/testimony_1297263844607.shtm, accessed 15 May 2011.
[487] (U) U.S. Census Bureau, Annual Estimates of the Population of Metropolitan and Micropolitan Statistical Areas: April 1, 2000 to July 1, 2009
[488] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed on 17 May 2011.
[489] (U) Global Terrorism Database, START, accessed on 17 May 2011
[490] (U) Goldman, Adam. "Saudi man charged with plotting terror attack researched Colorado dams," Denver Post, 24 February 2011, www.denverpost.com/breakingnews/ci_17472805, accessed 24 May 2011.
[491] (U//FOUO) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.
[492] (U) Federal Emergency Management Agency, www.fema.gov/news/disasters.fema, accessed 18 May 2011.
[493] (U) Federal Emergency Management Agency, National Emergency Management Information System, "FEMA Disaster Declarations Summary," "FEMA Hazard Mitigation, "FEMA Public Assistance Funded Projects Detail," and "FEMA Public Assistance Sub-grantee," all accessed on data.gov.
[494] (U) Ibid.
[495] (U) Federal Emergency Management Agency, *Region X,*www.fema.gov/about/regions/region, accessed 18 May 2011.
[496] (U) U.S. Geological Survey, Alaska Earthquake History, www.earthquake.usgs.gov/earthquakes/States/alaska/history.php, accessed 22 May 2011.
[497] (U) U.S. Geological Survey, Largest Earthquakes since 1900,www.earthquake.usgs.gov/earthquakes/world/10_largest_world.php, accessed 22 May 2011.
[498] (U) U.S. Geological Survey, Historic Earthquakes, www.earthquake.usgs.gov/earthquakes/States/events/1964_03_28.php, accessed 22 May 2011.
[499] (U) Washington Military Department, Emergency Management Division, www.emd.wa.gov/hazards/haz_earthquakes.shtml, accessed 22 May 2011.
[500] (U) U.S. Geological Survey, Seattle Seismic Hazard Maps and Data Download, www.earthquake.usgs.gov/regional/pacnw/hazmap/seattle, accessed 23 May 2011.
[501] (U) State of Alaska, State Homeland Security Strategy, 2009.
[502] (U//FOUO) Department of Homeland Security, Office of Intelligence and Analysis, "Washington: State Critical Infrastructure Threat Assessment, 2009.
[503] (U) Ibid.
[504] (U) Ibid.
[505] (U) U.S. Energy Information Administration, Alaska Quick Facts (2009), www.eia.gov/State/State-energy-profiles.cfm?sid=AK, accessed 23 May 2011.
[506] (U) State of Alaska, State Homeland Security Strategy, 2009.
[507] (U) U.S. Energy Information Administration, Alaska Quick Facts (2009), www.eia.gov/State/State-energy-profiles.cfm?sid=AK, accessed 23 May 2011.
[508] (U) Argonne National Laboratory, "Impacts from the Long-Term Closure of the Dalles Lock and Dam," 14 October 2009.
[509] (U) State of Oregon, "Situation Report1: Extended Navigation Lock Outage: Fuel Supply Impacts to Eastern Oregon," 27 September 2010, www.oregon.gov/ENERGY/NUCSAF/docs/Lock_Outage_SITREP1.pdf?ga=t, accessed 23 May 2010.
[510] (U) McFerron, Whitney, "U.S. Closing Columbia-Snake River System to Barges, May Curb Wheat Exports," Bloomberg News, 9 December 2010, www.bloomberg.com/news/2010-12-09/u-s-closing-columbia-river-to-barges-may-affect-wheat-exports.html, accessed 23 May 2010.
[511] (U) Based on searches of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Global Terrorism Database (GTD), www.start.umd.edu/gtd/, accessed on 17 May 2011.
[512] (U) Ibid.
[513] (U//FOUO) Department of Homeland Security, Office of Infrastructure Protection, National Critical Infrastructure Prioritization Program.