Table C-4. Scenarios Used for Insider Threat Risk Assessment

No.	Sector	Scenario Description
1	Food and Agriculture	Terrorism: An insider contaminates food processing plant via biological attack by introducing toxin into the U.S. milk supply. A 2005 Stanford University study pointed out that the milk industry's distribution systems are vulnerable to bioterrorism through the introduction of botulinum toxin, a deadly poison, into the milk supply. Based on the contamination of a single milk tanker and milk-processing facility, the toxin could be introduced to a large supply of milk via centralized storage and processing. This would dilute the toxin throughout several thousand gallons of milk and lead to widespread consequences.
2	Food and Agriculture	Terrorism: An insider contaminates food processing plant by introducing toxic chemical into the U.S. milk supply. Scenario No. 1 used as proxy for judgments on this scenario No. 2
3	Food and Agriculture	Terrorism: An insider contaminates beef in meat packing plant with E. coli O157 to create loss of confidence in food supply and nation-wide panic.
4	Food and Agriculture	Terrorism: An employee at a foot and mouth disease (FMD) biological-research center in the United States decides to circumvent on-site biosecurity measures to remove live FMD serotype from the facility and introduce it to multiple livestock feedlots and transport nodes in the U.S. "beef belt." This scenario has significant impact on the U.S. beef industry because of the specific serotype; the time elapsed from confirmation of the serotype, the number of animals exposed, and the push for emergency vaccinations.
5	Financial Services	Terrorism, Espionage, Corruption: An insider recruited by a foreign power or criminal organization to conduct cyberattack on an international financial system to disrupt international financial transactions and terrorist financial tracking
6	Financial Services	Terrorism, Corruption: A foreign organized crime group with links to a hostile nation-state coerces a financial clearing house employee, either on the software development or vulnerability management team, to attack the clearing house with the goal of creating massive capital flight from the United States. An insider interfering with time stamps on high-frequency trades could create a sudden liquidity crisis and a potential mini-market crash, thus having a potentially catastrophic impact on the U.S. economy.
7	Commercial Facilities	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. The employee learns that he or she will be let go by the company and decides to detonate a Vehicle-Born Improvised Explosive Device (VBIED) against the employer's place of business.
8	Communications	Terrorism: Insiders disrupt supply chain flow of Rare Earth Elements (REEs), which are critical components in cell phones and microwave and satellite communication systems. Insiders instigate political or trade disputes in the country of origin so that that nation purposely reduces or bans exports; or instigate labor strikes that halt the mining and processing of REEs. In 2008 a single foreign country supplied 96 percent of the U.S. imports of REEs; such a disruption in that country could potentially have significant consequences for the Communications Sector.
9	Critical Manufacturing	Terrorism: An insider at a major U.S. maritime port plants a powerful bomb that temporarily closes the port and the effects are felt throughout the CM Sector supply chain. U.S. maritime ports handle two billion tons of domestic and foreign cargo every year. The Critical Manufacturing (CM) Sector, in particular, relies on maritime ports for the import of raw materials, components, and finished products.
10	Dams	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. Employee learns he or she is going to be let go by the company and decides to detonate a large Improvised Explosive Device (IED) against a critical point in the dam's facility.
11	Energy	Terrorism: A foreign nation-state recruits an insider sympathetic to the foreign nation to carry out a sophisticated cyberattack on the automated control systems of a U.S. electrical transmission line.

No.	Sector	Scenario Description
12	Energy	Terrorism, Industrial Espionage: A foreign entity recruits an insider to provide essential information to enable them to engineer their hardware and embedded software products so that, once installed, they provide a "back door" for capturing and mapping real-time U.S. SCADA and "smart grid" system data. The information gained could be used to disrupt the system in time of conflict.
13	Government Facilities	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. The employee learns that he or she is going to be let go by the government and decides to detonate a VBIED against their employer's place of business.
14	Healthcare and Public Health	Terrorism, Corruption, Espionage: An insider disrupts supply chain flow of critical raw materials for health care equipment. Medical products and services rely on advanced technologies, such as nuclear technologies, that use rare raw materials from only a few suppliers. For example, the global isotope supply chain depends on a small number of aging nuclear reactors for isotope production and a complex processing and distribution chain for delivery of short-lived isotope products to the health care system. A disruption of the supply of the isotope Mo-99 could have significant impact on the global medical supply chain.
15	Healthcare and Public Health	Terrorism: Insider contaminates materials used in pharmaceutical production in an area that has a high concentration of pharmaceutical facilities. This disruption has a devastating effect on the U.S. supply of pharmaceuticals.
16	Healthcare and Public Health	Corruption/Organized Crime: A foreign-based organized crime organization uses insiders to facilitate its Medicare and Medicaid fraud activities in metropolitan centers in at least 20 States. This multinational criminal organization (MCO) is using traditional approaches including creating service providers and sham storefronts, etc. The MCO has recruited or placed insiders in a few major hospitals in the region, in regional Medicare Administrative Contractors, and in Centers for Medicare and Medicaid Services who are involved in claims and billing systems or who can facilitate processing fraudulent claims.
17	Information Technology	Terrorism: A foreign nation-state recruits an insider (with malicious intent after being hired) sympathetic to the foreign nation to attack U.S. electrical transmission lines.
18	Information Technology	Terrorism, Espionage, Corruption: Insider recruited by foreign power or criminal organization to conduct a cyberattack on an international financial system to disrupt international financial transactions and terrorist financial tracking.
19	Chemical and Transportation Systems	Terrorism: A foreign-based criminal organization recruits a criminal alien to detonate a truck containing chlorine inside a tunnel of a major metropolitan area.
20	Energy	Terrorism: A disgruntled employee causes an explosion on an offshore drilling rig in the Gulf of Mexico, resulting in the deaths of several workers, sinking of the drilling unit, an oil spill lasting three months, and various other economic, ecological, and health-related consequences.
21	Transportation Systems	Terrorism: A postal worker who is going to lose his or her job due to cutbacks at U.S. Postal Service (USPS) decides to get even with his employer by introducing an IED into the mail system. The worker has extensive knowledge of USPS air mail handling procedures and is able to circumvent existing countermeasures.
22	Transportation Systems	Terrorism, Corruption: A postal employee is recruited or coerced by an outside terrorist organization to introduce a biological agent into a postal facility. The employee receives financial rewards in exchange for his or her participation.
23	Transportation Systems	Terrorism: An airline pilot going through difficult personal time (e.g., financial troubles, divorce with intense custody battle) decides to deliberately crash the plane into a critical infrastructure asset.

No.	Sector	Scenario Description
24	Transportation Systems	Terrorism, Corruption: A baggage handler is a willing participant in a drug smuggling ring and had previously placed packaged thought to be carrying illegal drugs into the cargo hold of passenger aircraft. Unbeknownst to the baggage handler, the drug smuggling handlers are actually terrorists who eventually swap an explosive or bomb-making components for the "drug package" which then is placed in the cargo hold and detonated, resulting in the catastrophic loss of the aircraft.
25	Transportation Systems	Terrorism, Corruption: An airport screener is a willing participant in a drug smuggling ring and had previously allowed persons carrying drugs to pass through security checkpoints. Unbeknownst to the screener, the drug smuggling handlers are actually terrorists who eventually swap an explosive or bomb making components for the supposed drug package which then is allowed onto a passenger aircraft and results in the catastrophic loss of the aircraft.
26	Transportation Systems	Corruption: For financial gain, a field maintenance worker places an IED on section of pipeline to cause a double shear of pipe in a very remote location.
27	Transportation Systems	Terrorism: A disgruntled railroad employee with access to key bridges (e.g., maintenance worker, or mechanical engineer) deliberately causes mechanical failure at key vulnerable locations on railroad bridges.
28	Transportation Systems	Terrorism: A foreign nation recruits multiple insiders to conduct integrity attacks on rail control centers SCADA/scheduling systems (and other vectors) to delay U.S. military movement.
29	Transportation Systems	Terrorism: A terrorist group recruits an insider to assist with their successful wide-area biological/chemical attack on a major U.S. port. The attack kills or incapacitates the majority of the port's workforce and cripples the port's petrochemical complex and significantly disrupts the petrochemical industry. In addition, the port is closed for an indeterminate length of time, having a severe impact on its economic activity.
30	Border Security	Corruption: A drug cartel near the Southwest border of the United States recruits insiders who have access at border and operating nodes to facilitate expanding influence in United States, in order to gain access to rival group's territory and financial resources.
31	Water and Wastewater Systems	Terrorism: Terrorist group recruits insiders to inject lethal levels of fluoride into a municipal water treatment plant along the U.S. East Coast to disrupt the drinking water supply and to create panic.